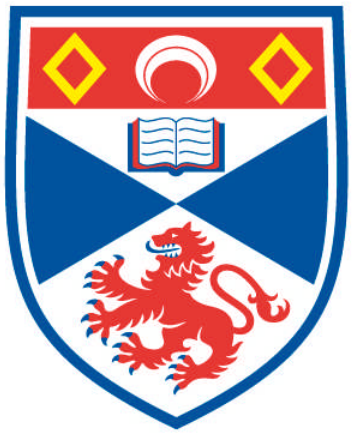
RANDOM GENERATION AND CHIEF LENGTH OF FINITE GROUPS

Nina E. Menezes

A Thesis Submitted for the Degree of PhD
at the
University of St Andrews



2013

Random generation and chief length of finite groups

Nina E. Menezes

A thesis submitted for the degree of Doctor of Philosophy at the University of St Andrews.
March 1, 2013

Abstract

Part I of this thesis studies $P_G(d)$, the probability of generating a non-abelian simple group G with d randomly chosen elements, and extends this idea to consider the conditional probability $P_{G,\mathrm{Soc}(G)}(d)$, the probability of generating an almost simple group G by d randomly chosen elements, given that they project onto a generating set of $G/\mathrm{Soc}(G)$. In particular we show that for a 2-generated almost simple group, $P_{G,\mathrm{Soc}(G)}(2) \geq 53/90$, with equality if and only if $G = A_6$ or S_6. Furthermore $P_{G,\mathrm{Soc}(G)}(2) \geq 9/10$ except for 30 almost simple groups G, and we specify this list and provide exact values for $P_{G,\mathrm{Soc}(G)}(2)$ in these cases. We conclude Part I by showing that for all almost simple groups $P_{G,\mathrm{Soc}(G)}(3) \geq 139/150$.

In Part II we consider a related notion. Given a probability ϵ, we wish to determine $d^{\epsilon}(G)$, the number of random elements needed to generate a finite group G with failure probabilty at most ϵ. A generalisation of a result of Lubotzky bounds $d^{\epsilon}(G)$ in terms of $l(G)$, the chief length of G, and $d(G)$, the minimal number of generators needed to generate G. We obtain bounds on the chief length of permutation groups in terms of the degree n, and bounds on the chief length of completely reducible matrix groups in terms of the dimension and field size. Combining these with existing bounds on $d(G)$, we obtain bounds on $d^{\epsilon}(G)$ for permutation groups and completely reducible matrix groups.

Candidate declarations

I, Nina Menezes, hereby certify that this thesis, which is approximately 75 000 words in length, has been written by me, that it is the record of work carried out by me and that it has not been submitted in any previous application for a higher degree.

I was admitted as a research student in September 2008 and as a candidate for the degree of Ph.D. in September 2009; the higher study for which this is a record was carried out in the University of St Andrews between 2008 and 2012.

Date:

Signature of candidate:

Supervisor declarations

I hereby certify that the candidate has fulfilled the conditions of the Resolution and Regulations appropriate for the degree of Ph.D. in the University of St Andrews and that the candidate is qualified to submit this thesis in application for that degree.

Date:

Signature of supervisor:

Permission for electronic publication

In submitting this thesis to the University of St Andrews I understand that I am giving permission for it to be made available for use in accordance with the regulations of the University Library for the time being in force, subject to any copyright vested in the work not being affected thereby. I also understand that the title and the abstract will be published, and that a copy of the work may be made and supplied to any bona fide library or research worker, that my thesis will be electronically accessible for personal or research use unless exempt by award of an embargo as requested below, and that the library has the right to migrate my thesis into new electronic forms as required to ensure continued access to the thesis. I have obtained any third-party copyright permissions that may be required in order to allow such access and migration, or have requested the appropriate embargo below.

The following is an agreed request by candidate and supervisor regarding the electronic publication of this thesis:

- Access to printed copy and electronic publication of thesis through the University of St Andrews.

Date:

Signature of candidate:

Signature of supervisor:

Acknowledgements

Most importantly I would like to thank my supervisors Dr. Martyn Quick and Dr. Colva Roney-Dougal. Without their knowledge, support and encouragement over the last four years, this thesis would not exist. I would also like to thank Dr. Eloisa Detomi & Prof. Andrea Lucchini for inviting to me to Padua on what proved to be a very productive research visit.

I would like to thank my friends for reminding me that there is a world outside of Maths and 'The Bubble'. My Maths Towers family have provided me with a lovely home during the Ph.D. 'journey'. In particular I would like to thank Si for providing Chocolate Oranges and Stella, and for laughing at my maths jokes. Jay has been the best office mate a girl could ask for; life will never be the same without 'The Cool Office'. I would also like to thank Kat, for ensuring that I was never homeless, and for saving me from slugs.

Finally I would like to thank my parents for instilling in me a love for learning, and my grandmother for her constant encouragement througout my education.

Contents

Chapter 1

Introduction

In this thesis we study two related questions concerning random generation of finite groups: probabilistic generation of almost simple groups, and the number of random elements required to generate a permutation or matrix group with a given probability.

In the first part of the thesis we study $P_G(d)$, the probability of generating a finite group G with d randomly chosen elements. Given a normal subgroup N we also study $P_{G,N}(d)$, the probability of generating a group G with d random elements, given that they project onto a generating set for the factor group G/N. In particular we study almost simple groups G with socle G_0. By the Classification of Finite Simple Groups all finite simple groups are 2-generated, and by [20], almost simple finite groups require at most 3 generators.

Dixon [22] proved that $P_{A_n}(2) \to 1$ as $n \to \infty$, settling a conjecture of Netto [75]. Further he conjectured that $P_G(2) \to 1$ as $|G| \to \infty$ for non-abelian simple groups G. This was proved by Kantor & Lubotzky for classical groups and some exceptional groups in [40], and settled for the remaining exceptional groups by Liebeck & Shalev [62]. These results are only concerned with the asymptotic behaviour of $P_G(2)$. We wish to find an explicit lower bound for $P_G(2)$. In fact we show that for 2-generated almost simple groups G, the probability $P_{G,G_0}(2) \geq 53/90 = 0.58\dot{8}$. Furthermore we show that $P_{G,G_0}(2) \geq 9/10$ except for 30 groups G which are listed together with the exact values of $P_{G,G_0}(2)$ in these cases. We estimate $P_{G,G_0}(2)$ below using maximal subgroup information and obtain explicit lower bounds on $P_{G,G_0}(2)$ for various families of non-abelian simple groups G_0. These bounds are given in terms of n if $G_0 = A_n$, in terms of n and q if G_0 is classical, and in terms of q if G_0 is exceptional, and are considered in Chapters 4, 5 and 6 respectively. As $P_{G,G_0}(3) \geq P_{G,G_0}(2)$, it can be shown without much further calculation that $P_{G,G_0}(3) \geq 139/150 = 0.92\dot{6}$. There are various applications of these results; we state two of them here.

Let $h_G(d)$ be the maximum h such that the direct product of h copies

of G can be generated by d elements. It was observed by Hall [32] that if S is a non-abelian simple group then

$$h_S(d) = \frac{P_S(d)|S|^{d-1}}{|\mathrm{Out}(S)|}.$$

Wiegold asks [71, Problem 17.116] for an explicit lower bound for $h_S(2)$, and in particular, whether $h_S(2) > \sqrt{|S|}$. It follows from our result that

$$h_S(2) \geq \beta\sqrt{S}$$

for $\beta = \frac{19}{\sqrt{60}}$ [73, Corollary 1.4]. We may also deduce an asymptotic result on $h_S(d)$ for $d \geq 2$ ([73, Theorem 1.3]), namely

$$h_S(d) \geq \alpha|S|^{d-1}/\log|S|,$$

where $\alpha = \frac{121}{1680}\log_2 20160$.

In [21] Detomi & Lucchini consider $P_{L,N}(d)$, where L is a finite group with a unique minimal normal subgroup N, and $d \geq d(L)$. They prove that if N is non-abelian, then $P_{L,N}(d) \geq 53/90$, and $P_{L,N}(d) \geq 8/10$ if L is not one of 8 specified groups. Our bounds on $P_{G,G_0}(2)$ for almost simple groups G are used in their proof.

In Part II we consider $d^\epsilon(G)$, the number of randomly chosen elements we require to generate a finite group G with failure probability at most ϵ. One use of these results is for the matrix group recognition project. When constructing composition trees for a permutation or matrix group, we construct homomorphisms ϕ, and generate subgroups $\mathrm{im}\,\phi$ and $\ker\phi$. Given ϕ it is easy to generate $\mathrm{im}\,\phi$ but harder to generate $\ker\phi$. Methods that always generate $\ker\phi$ take too long computationally. There are methods to generate random elements of a permutation or matrix group G, and thus it is useful for us to determine the number of random elements needed to generate G with a given probability. Note that the subgroups $\ker\phi$ are subnormal subgroups of the original permutation or matrix group we are given.

A generalisation of a result of Lubotzky [64] bounds $d^\epsilon(G)$ in terms of $d(G)$, the minimal number of generators required to generate G, and $l(G)$, the chief length of G. We are particularly interested in permutation and matrix groups for the applications described above. There are existing bounds on $d(G)$ in these cases; we seek bounds on $l(G)$.

In Chapter 9 we give some basic definitions and theorems on the chief length, together with more detail on Lubotzky's bounds on $d^\epsilon(G)$. We also state existing bounds on the minimal number of generators $d(G)$ from [13], [35], [47], [20], for G a permutation or matrix group. In Chapter 10 we bound the chief length of permutation groups in terms of the degree n, and give tighter bounds on $l(G)$ for primitive permutation groups G. Chapter

11 bounds the chief length of completely reducible matrix groups in terms of the degree n and field size q. We also obtain tighter bounds on $l(G)$ for G a weakly quasiprimitive matrix group. In both of these chapters the bounds on $l(G)$ are combined with existing bounds on $d(G)$ to obtain tighter upper bounds on $d^{\epsilon}(G)$.

Chapter 2

Preliminaries

First we discuss general definitions and notation. The following sections in this chapter discuss permutation groups, matrix groups, and finite simple groups in more detail. The final section in this chapter gives basic inequalities that will be used throughout this thesis. Throughout we will assume that all groups are finite unless otherwise stated (although some results do hold in the infinite case). Group actions and homomorphisms will be written on the right. Arbitrary groups of order n will be denoted by $[n]$, while n denotes the cyclic group C_n of order n. Logarithms will be taken to the base 2 unless stated otherwise.

Definition 2.0.1. Let A and B be groups. Then G is an *extension* of A by B if there exists $N \trianglelefteq G$ such that $N \cong A$ and $G/N \cong B$. Then G is denoted $A.B$. If there exists an $M \leq G$ such that $MN = G$, $M \cap N = 1$ and $M \cong B$, then this is a *split extension* and denoted $A : B$. We denote a non-split extension by $A^{\cdot}B$.

For simple groups G we may have more than one almost simple extension of G of the form $G.n$ for a given n. Then these extensions will be denoted $G.n_1$, $G.n_2$, etc., and these subscripts will correspond to the notation in the Atlas [17].

Definition 2.0.2. A group G is *almost simple* if it satisfies $S \cong \mathrm{Inn}(S) \leq G \leq \mathrm{Aut}(S)$ for some non-abelian simple group S.

Definition 2.0.3. Let $(H_i)_{i\in I}$ be a family of groups. Let G be a subgroup of the direct product $\prod_{i\in I} H_i$. Let $\pi_i : G \to H_i$ be the restriction to G of the projection map onto the i-th coordinate. Then G is a *subdirect product* of $(H_i)_{i\in I}$ if $G\pi_i = H_i$ for all $i \in I$.

Examples of subdirect products include direct products, and diagonal subgroups, as defined below.

Definition 2.0.4. Let G be a group, and let $\phi_2, \ldots, \phi_n \in \mathrm{Aut}(G)$. Then $D = \{(g, g^{\phi_2}, \ldots, g^{\phi_n}) \in G^n : g \in G\}$ is a *diagonal subgroup* of G^n.

Definition 2.0.5. Given a group G, the *Frattini subgroup*, $\Phi(G)$, is defined to be the intersection of all maximal subgroups of G.

Equivalently, $\Phi(G)$ is the set of all non-generators of G, that is, elements $g \in G$ such that if $G = \langle g, X \rangle$ then $G = \langle X \rangle$ for $X \subseteq G$.

Definition 2.0.6. An *elementary abelian group* is one where all non-trivial elements have order p for some prime p.

The notation p^n denotes an elementary abelian group of order p^n. This is not to be confused with the notation for a cyclic group. It should be clear from the context when we are talking about an elementary abelian p-group. Groups of the form $p^n.p^m$ may be denoted p^{n+m}.

Definition 2.0.7. The largest normal p-subgroup of a group G is the *p-radical* and is denoted $O_p(G)$.

Definition 2.0.8. A p-group G is an *extraspecial* group if $G' = Z(G) = \Phi(G) \cong C_p$.

It follows from this definition that $G/Z(G)$ is a non-trivial elementary abelian group. It can be shown that all extraspecial groups have order p^{1+2n} for some $n \geq 1$, and conversely, for each such number, there are exactly two extraspecial groups up to isomorphism. These subgroups are often denoted p_+^{1+2n} and p_-^{1+2n}.

Definition 2.0.9. A subgroup H of a group G is *p-local* if it is the normaliser of a non-trivial p-subgroup of G.

Definition 2.0.10. A subgroup H of G is *central* if $H \leq Z(G)$.

Definition 2.0.11. Let H and K be groups with subgroups $Z_1 \leq Z(H)$ and $Z_2 \leq Z(K)$, and let ϕ be an isomorphism from Z_1 to Z_2. Define $Z \leq H \times K$ by $Z = \{(x, x\phi) : x \in Z_1\}$. Then $G = (H \times K)/Z$ is a *central product* of H and K, denoted $H \circ K$. The groups H and K are *central factors* of G. If Z_1 and Z_2 are not specified, they are assumed to be the largest isomorphic subgroups of $Z(H)$ and $Z(K)$.

Definition 2.0.12. A subgroup H of a group G is a *characteristic subgroup* if $H^\phi = H$ for all $\phi \in \mathrm{Aut}(G)$ and it is denoted $H \operatorname{char} G$.

Definition 2.0.13. A group G is *characteristically simple* if it has no proper non-trivial characteristic subgroups, that is, no proper non-trivial subgroups which are invariant under $\mathrm{Aut}(G)$.

Lemma 2.0.14. *Let G be characteristically simple. Then G is the direct product of isomorphic simple groups.*

Proof. Let S be a minimal normal subgroup of G. Let

$$\mathcal{S} = \{N \trianglelefteq G : N = S_1 \times S_2 \times \cdots \times S_k, S_i \text{ minimal normal}, S_i \cong S\}.$$

As $S \in \mathcal{S}$, this set contains non-trivial subgroups of G. Choose $N \in \mathcal{S}$ of largest possible order. Then $N = S_1 \times \cdots \times S_k$ for some $k \geq 1$.

First we show that $N = G$. Suppose for a contradiction that N is not equal to G. As G is characteristically simple, N cannot be a characteristic subgroup of G. Hence there exists some $\phi \in \mathrm{Aut}(G)$ such that $N\phi \nleq N$. Thus there exists S_i such that $S_i\phi \nleq N$. As ϕ is an automorphism of G, $S_i\phi$ is a minimal normal subgroup of G. Then $N \cap S_i\phi \trianglelefteq G$. As $S_i\phi \nleq N$, then $N \cap S_i\phi \neq S_i\phi$. The minimality of S_i implies that $N \cap S_i\phi = 1$. It follows that

$$N \times S_i\phi = S_1 \times \cdots \times S_k \times S_i\phi \trianglelefteq G.$$

This contradicts the maximality of N in $\mathcal{S}$. Then $G = N$, the direct product of subgroups isomorphic to a minimal normal subgroup S.

It remains to show that S is simple. Let K be a normal subgroup of S. Then K is also normal in G. The minimality of S in G implies that $K = 1$ or S. Thus S is simple as required. □

Then a characteristically simple group is either the direct product of isomorphic non-abelian simple groups or it is elementary abelian.

Definition 2.0.15. Let H be a subgroup of a group G. If there exists a series $H = H_0 \lhd H_1 \lhd \ldots \lhd H_n = G$, then H is a *subnormal* subgroup of G and this is denoted $H \lhd\lhd G$.

Note that we may have $n = 0$, that is, G is a subnormal subgroup of itself.

Definition 2.0.16. A group is *perfect* if it equals its own commutator subgroup.

Definition 2.0.17. A *central extension* of a group G is a pair (H, π) where H is a group and $\pi : H \to G$ is a surjective homomorphism such that $\ker \pi \leq Z(H)$. We may also refer to H as a *central extension* of G.

Definition 2.0.18. A *perfect central extension* or *covering* of a perfect group G is a central extension (H, π) of G with H perfect.

Definition 2.0.19. A *morphism* $\alpha : (G_1, \pi_1) \to (G_2, \pi_2)$ of central extensions of G is a group homomorphism $\alpha : G_1 \to G_2$ with $\pi_1 = \alpha\pi_2$.

Definition 2.0.20. A central extension $(\tilde{G}, \pi)$ of G is *universal* if for each central extension (H, σ) of G there exists a unique morphism $\alpha : (\tilde{G}, \pi) \to (H, \sigma)$ of central extensions.

Lemma 2.0.21 ([1, (33.1)])**.** *Up to isomorphism there is at most one universal central extension of a group G.*

Proof. Suppose (G_1, π_1) and (G_2, π_2) are universal central extensions of G. Then, as they are universal, there exist morphisms of central extensions $\alpha_1 : (G_1, \pi_1) \to (G_2, \pi_2)$ and $\alpha_2 : (G_2, \pi_2) \to (G_1, \pi_1)$. Then we have morphisms $\alpha_1\alpha_2 : (G_1, \pi_1) \to (G_1, \pi_1)$ and $\alpha_2\alpha_1 : (G_2, \pi_2) \to (G_2, \pi_2)$. Uniqueness of such morphisms tell us that $\alpha_1\alpha_2 = 1 = \alpha_2\alpha_1$. Then α_1, $\alpha_2 = \alpha_1^{-1}$ are isomorphisms and the result follows. □

Theorem 2.0.22 ([1, (33.4)])**.** *G possesses a universal central extension if and only if G is perfect.*

Definition 2.0.23. If G is a perfect group with $(\tilde{G}, \pi)$ its universal central extension, then $\tilde{G}$ is the *universal covering group* or *full covering group* of G and $\ker \pi = M(G)$ is the *(Schur) multiplier* of G.

The orders of the Schur multipliers of simple groups are listed in the Atlas [17].

Definition 2.0.24. A *quasisimple group* is a perfect group G such that $G/Z(G)$ is a non-abelian simple group.

So quasisimple groups are perfect central extensions of simple groups.

Definition 2.0.25. Let G be a group.

- The *Fitting subgroup* of G, denoted $F(G)$, is the largest nilpotent normal subgroup of G.
- The *components* of G are its subnormal quasisimple subgroups.
- The *layer* of G, $E(G)$, is the subgroup generated by the components of G.
- The *generalised Fitting subgroup* of G is $F^*(G) = F(G)E(G)$.

Lemma 2.0.26 ([1, (31.8), (31.7), (31.12)])**.** *Let G be a group. Then*

- *$F(G)$ is the direct product of the groups $O_p(G)$ for all prime divisors p of $|G|$;*
- *$E(G)$ is a central product of the components of G;*
- *$F^*(G)$ is a central product of $F(G)$ with $E(G)$.*
- *$C_G(F^*(G)) \leq F^*(G)$.*

Thus $F^*(G)$ is a central product of groups $O_p(G)$ for all prime divisors p of $|G|$, and the subnormal quasisimple subgroups of G.

2.1 Permutation groups

Denote the symmetric group acting on a set Ω by $\mathrm{Sym}(\Omega)$. If $|\Omega| = n$, then it may be denoted $\mathrm{Sym}(n)$ or S_n. The corresponding alternating groups are denoted $\mathrm{Alt}(\Omega)$, $\mathrm{Alt}(n)$ or A_n.

Definition 2.1.1. A *permutation group* is a subgroup G of S_n. The *degree* of G is n.

Definition 2.1.2. A homomorphism $\rho : G \to S_n$ is a *permutation representation* of G.

Definition 2.1.3. Let G be a group and Ω a set. A *group action* of G on Ω is a map $\mu : \Omega \times G \to G$ satisfying the following:

1. $\mu(x, gh) = \mu(\mu(x, g), h)$ for $g, h \in G$, $x \in \Omega$,
2. $\mu(x, 1) = x$ for $x \in \Omega$.

Then we say that Ω is a *G-space*. We usually write xg (or sometimes x^g) for $\mu(x, g)$.

One example of group actions is the action of G on the cosets of some subgroup $H \leq G$. In this case Ω is the set of right cosets of H, and G acts on Ω via multiplication on the right.

Definition 2.1.4. Let a group G act on sets Ω and Ω'. Suppose f is a bijection from Ω to Ω'. If $(xg)f = (xf)g$ for all $x \in \Omega$ and $g \in G$, then these actions are *G-isomorphic*.

If G acts on a set Ω, then this corresponds to a permutation representation of G of degree $n = |\Omega|$ where we define the representation $\rho : G \to S_n$ by $x(g\rho) = xg$ for all $g \in G$, $x \in \Omega$. Conversely, a permutation representation $\rho : G \to S_n$ gives a group action if we define $xg = x(g\rho)$ for $x \in \Omega$, $g \in G$. If we have a faithful representation, that is, $\ker \rho = 1$, then G embeds in S_n. Note that all non-trivial permutation representations of a simple group G are faithful as $\ker \rho$ is a normal subgroup of G.

Definition 2.1.5. A group G acts on itself via right multiplication. This is the *(right) regular representation*.

From this representation we obtain the following.

Theorem 2.1.6 (Cayley's Theorem)**.** *Every group G can be embedded in the symmetric group on G.*

Definition 2.1.7. Let G be a group acting on a set Ω.

- For $x \in \Omega$, the *orbit* of x is the set $\{x^g : g \in G\}$. The *stabiliser* of x is the set $\{g : x^g = x\}$, which is denoted G_x.

- G is *transitive* if it has only one orbit, otherwise it is *intransitive*.
- A transitive group G acting on a set Ω is said to act *regularly* if $G_x = 1$ for each $x \in \Omega$.

If G is an intransitive group, then it can be described in terms of its action on each of its orbits.

Theorem 2.1.8 ([11, Theorem 1.2]). *Let G be an intransitive group acting on Ω, with orbits $\Omega_1, \Omega_2, \ldots, \Omega_k$. Let G_i be the image of the associated permutation representation $G \to \mathrm{Sym}(\Omega_i)$. Then G is a subdirect product of the groups $G_1, G_2, \ldots, G_k$.*

The Orbit–Stabiliser Theorem is well known.

Theorem 2.1.9 (Orbit–Stabiliser Theorem). *Let G be a group acting on a set Ω. If x^G denotes the orbit of x, then $|x^G| = [G : G_x]$.*

It follows that a group G acts regularly on a set Ω if and only if $|G| = |\Omega|$.

Definition 2.1.10. Let G be a transitive group acting on a set Ω.

- A set $\Delta \subseteq \Omega$ is a *block* for G if for all $g \in G$, either $\Delta^g = \Delta$ or $\Delta^g \cap \Delta = \emptyset$.
- $\Delta = \Omega$ and $\Delta = \{x\}$ for $x \in \Omega$ are the *trivial blocks*.
- If G has a set of non-trivial blocks then it is *imprimitive*, otherwise it is *primitive*.

Theorem 2.1.11 ([11, Theorem 1.3, Theorem 1.7]). *Let G act transitively on Ω, and let H and K be subgroups of G.*

- *The action of G on Ω is G-isomorphic to the action of G on the set of right cosets of G_α for $\alpha \in \Omega$.*
- *The action of G on the set of right cosets of H and the action of G on the set of right cosets of K are G-isomorphic if and only if H and K are conjugate subgroups of G.*
- *G is primitive if and only if G_α is a maximal subgroup of G.*

Then primitive permutation representations of G correspond to conjugacy classes of maximal subgroups of G. It follows that the minimal degree of a non-trivial permutation representation of a group G corresponds to the minimum index of a proper subgroup H of G. The minimal degree of a non-trivial permutation representation of a simple group G is known. If $G = A_n$, then the minimal degree is n; if G is classical the degrees are given in [18] (with corrections in [44] and [9]); if G is exceptional the degrees are given in ([89], [88] and [90]); and if G is sporadic then the minimal degrees are given in the Atlas [17]. These will be useful later when we need to estimate the indices of maximal subgroups.

Definition 2.1.12. Two permutation subgroups $G \leq \mathrm{Sym}(\Omega)$ and $H \leq \mathrm{Sym}(\Omega')$ are *permutation isomorphic* if there exists a bijection $f : \Omega \to \Omega'$ and an isomorphism $\theta : G \to H$ such that for $g \in G$ and $x \in \Omega$, $(x^g)f = (xf)^{(g\theta)}$.

This means that G and H are 'the same' up to relabelling of the points. Permutations in S_n are conjugate if and only if they have the same cycle type. Then G and H are permutation isomorphic subgroups of S_n if and only if they are conjugate in S_n.

Definition 2.1.13. Let H and K be groups, and let $\phi : H \to \mathrm{Aut}(K)$ be a homomorphism. Then the *semidirect product* of H and K (with respect to ϕ) is the set $H \times K$ with multiplication defined by $(h_1, k_1)(h_2, k_2) = (h_1h_2, k_1^{h_2\phi}k_2)$ for $h_i \in H$, $k_i \in K$. This group is denoted $K \rtimes_\phi H$.

It can be shown that if a group $G = HK$, for $H \leq G$, $K \trianglelefteq G$ and $H \cap K = 1$, then $G \cong K \rtimes H$. Then semidirect products are precisely the split extensions of H by K.

Definition 2.1.14. Let K and H be groups where H acts on a non-empty set Γ. Then the *wreath product* of K by H with respect to this action is the semidirect product $K^\Gamma \rtimes H$, where K^Γ is the set of all the functions $\Gamma \to K$ (as K is a group, this is a group under pointwise multiplication). Here H acts on K^Γ via $f^x(\gamma) = f(\gamma^{x^{-1}})$ for $f \in K^\Gamma$, $\gamma \in \Gamma$, $x \in H$. The group $K^\Gamma \rtimes H$ is denoted $K \,\mathrm{wr}_\Gamma\, H$,

We get different groups for different actions of H. If the action is not specified and $H \leq \mathrm{Sym}(t)$, then we consider the wreath product $K^t \rtimes H$, where H permutes the coordinates of K^t. Otherwise, if the action is not specified, then we assume that H has the regular action.

If K acts on a set Δ and H acts on Γ, then we can define an action of $W = K\mathrm{wr}_\Gamma H$ on $\Delta \times \Gamma$ by $(\delta, \gamma)^{(f,u)} = (\delta^{f(\gamma)}, \gamma^u)$ for all $(\delta, \gamma) \in \Delta \times \Gamma$ where $(f, u) \in W$. If $|\Delta| > 1$ and $|\Gamma| > 1$ then this action is imprimitive. Conversely, given an imprimitive group $G \leq \mathrm{Sym}(\Omega)$, with blocks $\Delta_1, \ldots, \Delta_k$, we may embed G into a wreath product. Let $G_{\{\Delta_1\}}$ be the setwise stabiliser of Δ_1, and let $G_{(\Delta_1)}$ be the pointwise stabiliser of Δ_1. Then $G_{\{\Delta_1\}}/G_{(\Delta_1)}$ is the group of permutations induced by the action of $G_{\{\Delta_1\}}$ on Δ_1, and this is independent of the choice of Δ_1. Then G embeds into a wreath product as follows.

Theorem 2.1.15 ([6, Theorem 8.5])**.** *Let G be an imprimitive group acting on blocks $\Delta_1, \ldots, \Delta_k$. Let K be the group induced by G which permutes the blocks, and let $H = G_{\{\Delta_1\}}/G_{(\Delta_1)}$. Then $G \leq H \,\mathrm{wr}\, K$.*

We prove the following lemma for imprimitive groups.

Lemma 2.1.16. *Let G be an imprimitive group acting on blocks $\Delta_1, \ldots, \Delta_k$. Then G can be considered as a subgroup of $H \operatorname{wr} K$, where H is the group induced by the action of $G_{\{\Delta_1\}}$ on Δ_1, and K is the group induced by the action of G permuting the blocks. Then $(H^k \cap G)$ is a normal subgroup of G, and $(H^k \cap G)$ is a subdirect product of N^k for some $N \trianglelefteq H$.*

Proof. As $H^k = H_1 \times \cdots \times H_k$ is normal in $H \operatorname{wr} K$, then $H^k \cap G$ is normal in G. Next we show that $H^k \cap G$ is a subdirect product of some normal subgroup of H. For $1 \leq i \leq k$ let $\pi_i : G_{\{\Delta_i\}} \to H_i$ be the projection map from $G_{\{\Delta_i\}}$ to the ith copy of H. Let $N = (H^k \cap G)\pi_1$. Note that $G_{\{\Delta_i\}}\pi_i = H$. Then as

$$H^k \cap G \trianglelefteq G_{\{\Delta_1\}} \leq G,$$

N is normal in H.

Pick $h = (h_1, \ldots, h_k)1 \in H^k \cap G$. As K is transitive on the set of blocks, there exists $x \in G$ where $x = (x_1, \ldots, x_k)\sigma$ for $\sigma \in K$ such that $i\sigma = 1$. Then

$$x^{-1}hx = (x_1^{-1}h_{1\sigma^{-1}}x_1, \ldots, x_k^{-1}h_{k\sigma^{-1}}x_k)1 \in H^k \cap G.$$

It follows that $(H^k \cap G)\pi_i = N^y \cong N$ for some $y \in H$. The normality of N in H implies $N^y = N$.

Then $(H^k \cap G)\pi_i \cong N$. Also $H^k \cap G \leq (H_k \cap G)\pi_1 \times \ldots \times (H_k \cap G)\pi_k \cong N^k$. So $(H^k \cap G)$ is a subdirect product of N^k as required. □

We can also define a primitive action for the wreath product as follows.

Definition 2.1.17. Let H and K be groups acting on Γ and Δ respectively. Let Δ^Γ be the set of all functions from Γ to Δ. Let W be the wreath product $K \operatorname{wr}_\Gamma H$. For each $\phi \in \Delta^\Gamma$ and $(f, x) \in W$, define the action of W on Δ^Γ by $\phi^{(f,x)}(\gamma) = \phi(\gamma^{x^{-1}})^{f(\gamma^{x^{-1}})}$. This is the *product action* of $K \operatorname{wr}_\Gamma H$ on Δ^Γ.

Under certain conditions this product action is primitive as described in [24].

Lemma 2.1.18 ([24, Lemma 2.7A])**.** *Suppose that K and H are non-trivial groups acting on the sets Γ and Δ, respectively. Then the wreath product $K \operatorname{wr}_\Gamma H$ is primitive in the product action on Δ^Γ if and only if:*

1. *K acts primitively but not regularly on Δ; and*
2. *Γ is finite and H acts transitively on Γ.*

Definition 2.1.19. Let F be a field. The *affine geometry* $\mathrm{AG}_d(F)$ consists of points and affine subspaces constructed from the vector space F^d. The points of the geometry are the vectors of F^d. If S is a k-dimensional vector subspace of F^d, then the set $S + x = \{v + x : v \in S\}$ is an affine subspace of dimension k for every $x \in F^d$. That is, the affine subspaces are translates of the vector subspaces of F^d.

Definition 2.1.20. An *affine transformation* is an automorphism of the affine geometry of the form

$$\begin{aligned} t_{A,v} : F^d &\to F^d \\ u &\mapsto uA + v \end{aligned}$$

where $A \in \mathrm{GL}_d(F)$ and $v \in F^d$. The set of all affine transformations forms the *affine general linear group*, denoted $\mathrm{AGL}_d(F)$. If F is a finite field with q elements, then we may write $\mathrm{AGL}_d(q)$.

The group $\mathrm{GL}_d(F)$ will be discussed further in the following section. The set of translations $T = \{t_{1,v} : v \in F^d\}$ is a normal subgroup of $\mathrm{AGL}_d(F)$ and is isomorphic to F^d (considered as a group under addition). The affine general linear group is a split extension of T by a subgroup isomorphic to $\mathrm{GL}_d(F)$. Here the action of $\mathrm{GL}_d(F)$ on T is matrix multiplication.

Definition 2.1.21. A permutation group is of *affine type* if it is a subgroup of an affine general linear group and it contains the subgroup of translations T.

Definition 2.1.22. Let T be a non-abelian simple group. A permutation group G is of *diagonal type* if $T^k \leq G \leq T^k.(\mathrm{Out}(T) \times S_k)$ and G acts as described below. The symmetric group S_k acts on T^k by permuting the coordinates. For $(t_1, t_2, \ldots, t_k) \in T^k$ and $\tau \in \mathrm{Out}(T)$, the group $\mathrm{Out}(T)$ acts on T^k via $(t_1, t_2, \ldots, t_k)^\tau = (t_1^\tau, t_2^\tau, \ldots, t_k^\tau)$. The diagonal subgroup of T^k is defined to be $D = \{(t, t, \ldots, t) : t \in T\}$ and is isomorphic to T. Then $G = T^k.L$ for some $L \leq \mathrm{Out}(T) \times S_k$ and G acts on the (right) cosets of $D.L$ (the normaliser of D in G) by right multiplication.

The next groups we define are twisted wreath products. Let T, K be arbitrary groups and recall T^K is the set of functions from K to T. This forms a group under pointwise multiplication. We give a brief definition here which will be sufficient for our requirements, for more detail see [24, Section 4.7].

Definition 2.1.23. Let T and K be arbitrary groups, and let L be a subgroup of K with a specified homomorphism $\phi : L \to \mathrm{Aut}(T)$. Define an action of K on T^K via

$$f^x(z) = f(xz)$$

for $x, z \in K$. Let

$$H = \{f \in T^K : f(zy) = f(z)^{y\phi} \text{ for } z \in K, y \in L\} \leq T^K.$$

Then we may define the semidirect product $G = H \rtimes K$. This is the *twisted wreath product* with respect to the data (T, K, ϕ).

It can be shown that $H \cong T^m$ where $m = [K : L]$. Any finite primitive group G with regular non-abelian socle is isomorphic to a twisted wreath product where $G = T^m.G_\alpha$, where T is a non-abelian simple group, the point stabiliser G_α is a subgroup of S_m, and G acts primitively on $|T|^m$ points. The twisted wreath product of smallest degree acts on 60^6 points.

The O'Nan–Scott Theorem was proved independently by O'Nan and Scott, and published in [85, Appendix]. The original version describes maximal subgroups of A_n or S_n. Note that this version excludes twisted wreath products as they are not maximal [11, Section 4.6].

Other versions of the O'Nan–Scott Theorem describe primitive permutation groups. We have stated two versions here that are easiest for us to work with.

The following is the O'Nan–Scott Theorem (as stated in [53]) which will allow us to determine the maximal subgroups of A_n.

Theorem 2.1.24 (O'Nan–Scott)**.** *If G is A_n or S_n and M is any maximal subgroup of G other than A_n, then M is one of the following.*

1. *M is intransitive, $M = (S_k \times S_m) \cap G$ with $n = k + m$, $m \neq k$.*
2. *M is imprimitive, $M = (S_m \operatorname{wr} S_k) \cap G$ with $n = mk$, $m > 1$ and $k > 1$.*
3. *M is primitive and is one of the types below.*
   - *Affine type: $M = \mathrm{AGL}_k(p) \cap G$, $n = p^k$ for some prime p.*
   - *Diagonal type: $M = (T^k.(\mathrm{Out}(T) \times S_k)) \cap G$ where T is a non-abelian simple group, $k \geq 2$ and $n = |T|^{k-1}$.*
   - *Product action type: $M = (S_m \operatorname{wr} S_k) \cap G$ with the product action, where $n = m^k$, $m \geq 5$ and $k > 1$.*
   - *Almost simple: $T \leq M \leq \mathrm{Aut}(T)$ where T is a non-abelian simple group, $T \neq A_n$.*

Not all these subgroups M are maximal, but [53] determines which of these possibilities M are maximal in G. If $G = S_n$, it follows from the original statement of the O'Nan–Scott Theorem in [85] that for all of these groups apart from the almost simple subgroups, there is one conjugacy class of each type of maximal subgroup for each k (or one for each k and T in the case of diagonal type subgroups).

Next we state the version from [24] which describes all primitive permutation groups.

Theorem 2.1.25 (O'Nan–Scott)**.** *Let G be a finite primitive group of degree n and let $H = \mathrm{Soc}(G)$. Then $H \cong T^k$ for some simple group T. If H is regular then one of the following holds.*

1. *G is of affine type: H is an elementary abelian p-group, $n = p^k$ and G is isomorphic to $\mathbb{F}_p^k \rtimes K$ for some irreducible subgroup $K \leq \mathrm{GL}_k(p)$.*

2. *G is a twisted wreath product: H and T are non-abelian, $n = |T|^k$ for some $k \geq 6$ and $G = H.K$ for some transitive subgroup $K \leq S_k$.*

If H is not regular then T is non-abelian and one of the following holds.

3. *G is almost simple: H is simple and $H \leq G \leq \mathrm{Aut}(H)$.*

4. *G is of diagonal type: $H = T^k$ for $k \geq 2$, $n = |T|^{k-1}$ and $T^k \leq G \leq T^k.(\mathrm{Out}(T) \times S_k)$.*

5. *G is of product type: $H = T^k$ with $k = rs$ for $s > 1$ and $G \leq U \operatorname{wr} S_s$ for some primitive group U of degree d. The group U is almost simple or of diagonal type and $n = d^s$.*

2.2 Matrix groups

Definition 2.2.1. The *general linear group* $\mathrm{GL}(V)$ is the group of invertible linear maps from V to itself.

This group can be thought of as the set of all invertible n by n matrices over the field F, and so we may write $\mathrm{GL}(V) = \mathrm{GL}_n(F)$. Finite fields F all have order q for some prime power q, all finite fields of order q are isomorphic, and we may denote this group $\mathrm{GL}_n(q)$.

Definition 2.2.2. Let $G \leq \mathrm{GL}(V)$. Then G is a *linear group* or a *matrix group*.

The following is well known.

Proposition 2.2.3. *The order of $\mathrm{GL}_n(q)$ is*

$$q^{n(n-1)/2} \prod_{i=1}^{n} (q^i - 1).$$

Proof. The group $\mathrm{GL}_n(q)$ acts regularly on the set of ordered bases of $\mathbb{F}_q^n$ so to determine the order of the group we count the number of ordered bases. Then

$$\begin{aligned} |\mathrm{GL}_n(q)| &= (q^n - 1)(q^n - q) \dots (q^n - q^{n-1}) \\ &= q^{n(n-1)/2} \prod_{i=1}^{n} (q^i - 1). \end{aligned}$$

□

Recall the definition of the affine general linear group from the previous section. We now state its order.

Lemma 2.2.4. *The order of* $\mathrm{AGL}_d(q)$ *is* $q^d \prod_{i=0}^{d-1}(q^d - q^i)$.

Proof. As $\mathrm{AGL}_d(q)$ is the split extension of $\mathbb{F}_q^d$ and $\mathrm{GL}_d(q)$ its order is $q^d \times \prod_{i=0}^{d-1}(q^d - q^i)$. □

Definition 2.2.5. Let $\rho : G \to \mathrm{GL}_n(F)$ be a group homomorphism. Then ρ is a *(matrix) representation* of G. We define an action of G on the vector space $V = F^n$ by $vg = v(g\rho)$ for $v \in V$, $g \in G$. Then V is an *FG-module*. A subspace $U \leq V$ is an *FG-submodule* if U is invariant under the action of G.

Definition 2.2.6. Let V and W be FG-modules. A function $\theta : V \to W$ is an *FG-homomorphism* if θ is a linear transformation and $(vg)\theta = (v\theta)g$ for all $v \in V$, $g \in G$. If θ is invertible then this is an *FG-isomorphism* and we write $V \cong W$.

Definition 2.2.7. Two representations $\rho : G \to \mathrm{GL}_n(F)$ and $\sigma : G \to \mathrm{GL}_n(F)$ are *equivalent* if and only if there exists a matrix $P \in \mathrm{GL}_n(F)$ such that $P^{-1}(g\rho)P = g\sigma$ for all $g \in G$.

It can be shown that ρ, σ are equivalent if and only if the representations ρ and σ have isomorphic modules.

Similarly we may define projective representations.

Definition 2.2.8. Let $\rho : G \to \mathrm{PGL}_n(F)$ be a group homomorphism. Then ρ is a *projective representation* of G.

If we have a faithful representation $\rho : G \to \mathrm{GL}_n(F)$ then we may consider G as a subgroup of $\mathrm{GL}_n(F)$. We will consider this case for the rest of this section as we are interested in matrix groups. If ρ is any representation (not necessarily faithful), then there are similar definitions for ρ to be reducible, irreducible, etc.

Definition 2.2.9. Let $G \leq \mathrm{GL}_n(F)$ and let $V = F^n$.

- V is the *natural module* for G.
- G is *reducible* if there is a G-invariant subspace U of V other than $\{0\}$ and V. Otherwise G is *irreducible*. Then V is respectively a *reducible* or *irreducible* FG-module.
- If V can be expressed as the direct sum of subspaces $V_1, \ldots, V_k$, where G acts irreducibly on each V_i, then G is *completely reducible*. Each V_i is a *constituent* of the module V.

- If $G \leq \mathrm{GL}_n(F)$ is irreducible as a subgroup of $\mathrm{GL}_n(K)$ for any field extension K of F, then G is *absolutely irreducible*.
- The field F is a *splitting field* for G if every irreducible representation of G over F is absolutely irreducible, and F is minimal with this property.

We will often need to consider absolutely irreducible representations of groups and will use the following.

Definition 2.2.10. Let F_1 be an extension field of the field F. Then the *Galois group*, $\mathrm{Gal}(F_1/F)$, is the group of all field automorphisms of F_1 that leave all elements of F fixed.

If $F = \mathbb{F}_q$ and $F_1 = \mathbb{F}_{q^s}$, then $\mathrm{Gal}(F_1/F)$ is cyclic of order s.

Theorem 2.2.11 ([36, Theorem 9.2])**.** *Let $G \leq \mathrm{GL}_n(F)$ be irreducible. The following are equivalent.*

1. *G is absolutely irreducible.*
2. *$C_{\mathrm{GL}_n(F)}(G)$ consists of scalar matrices.*

The next theorem is a consequence of [36, Theorem 9.21 & Corollary 9.22].

Theorem 2.2.12. *Let $G \leq \mathrm{GL}_n(F)$ be irreducible, and let E be a splitting field for G such that $F \leq E$.*

1. *G is completely reducible when considered as a subgroup of $\mathrm{GL}_n(E)$.*
2. *There exists a field F_1, with $F \leq F_1 \leq E$ and $[F_1 : F] = f$, such that G embeds irreducibly in $\mathrm{GL}_{n/f}(F_1)$.*

As with permutation groups, we have the notion of imprimitive and primitive matrix groups.

Definition 2.2.13. Let $G \leq \mathrm{GL}_n(F)$ and let $V = F^n$.

- Let G be irreducible. If G preserves some direct sum decomposition $V = V_1 \oplus V_2 \oplus \cdots \oplus V_t$ for $t > 1$, then G is *imprimitive*, otherwise G is *primitive*.
- G is *homogeneous* if G is completely reducible with $V = V_1 \oplus \ldots \oplus V_t$ for V_i irreducible and $V_1 \cong V_i$ for $1 \leq i \leq t$. In this case we say that G acts *homogeneously* on V.
- G is *quasiprimitive* if all of its normal subgroups are homogeneous.
- G is *weakly quasiprimitive* if all of its characteristic subgroups are homogeneous.

Note that a primitive group is quasiprimitive, otherwise the homogeneous components of some normal subgroup would form an imprimitive sum decomposition for V.

Definition 2.2.14. Let V and W be vector spaces over a field F. Let T be an F-vector space together with a bilinear map $\tau : V \times W \to T$. Then T is a *tensor product* of V and W if, whenever we have a bilinear map $\phi : V \times W \to U$, there exists a $\bar{\phi} : T \to U$ such that $\phi = \tau\bar{\phi}$.

It can be shown that tensor products exist and are unique up to isomorphism, and we denote T by $V \otimes W$. If V and W are vector spaces with bases $\{v_1, \ldots, v_k\}$ and $\{w_1, \ldots, w_m\}$ respectively, then $V \otimes W$ is the km-dimensional vector space over F with basis given by $\{v_i \otimes w_j : 1 \leq i \leq k, 1 \leq j \leq m\}$.

Let G be the direct product of groups H and L. Using the notation above, let V and W be FH- and FL-modules respectively. Then $U = V \otimes W$ can be considered as an FG-module where the action is as follows. For $g \in G$, $g = hl$ for some unique $h \in H$ and $l \in L$. Then g acts on basis vectors $v_i \otimes w_j$ of U via

$$(v_i h \otimes w_j l)$$

and extending this action to all of U by linearity. It can be shown that U is an irreducible FG-module if and only if V and W are irreducible FH- and FL-modules respectively.

2.2.1 Classical groups

The classical groups comprise linear, symplectic, unitary and orthogonal groups, all of which will be defined in this section. All the definitions and theorems in this section come from [17], [44] and [87], where more details can be found. We are particularly interested in simple classical groups. First we consider the general linear group $\mathrm{GL}_n(F) = \mathrm{GL}(V)$ and define the related semilinear group, and associated subgroups and quotient groups.

Definition 2.2.15. A map $g : V \to V$ is a *semilinear transformation* of a vector space $V = F^n$ if there exists a field automorphism $\sigma \in \mathrm{Aut}(F)$ such that for all $v, w \in V$, $\lambda \in F$,

$$(v + w)g = vg + wg \text{ and } (\lambda v)g = \lambda^\sigma (vg).$$

A semilinear transformation g is *non-singular* if $vg = 0$ implies $v = 0$. The set of all non-singular semilinear transformations of V forms a group $\Gamma\mathrm{L}(V) = \Gamma\mathrm{L}_n(F)$, the *general semilinear group* of V.

Definition 2.2.16. The *special linear group*, $\mathrm{SL}_n(F)$, is the set of all elements of $\mathrm{GL}_n(F)$ with determinant 1.

Groups	Index	Groups	Index
$[\Gamma\mathrm{L}_n(q) : \mathrm{GL}_n(q)]$	f	$[\mathrm{P}\Gamma\mathrm{L}_n(q) : \mathrm{PGL}_n(q)]$	f
$[\mathrm{GL}_n(q) : \mathrm{SL}_n(q)]$	$q-1$	$[\mathrm{PGL}_n(q) : \mathrm{PSL}_n(q)]$	$(n, q-1)$

Table 2.1: Indices of subgroups of $\Gamma\mathrm{L}_n(q)$ and $\mathrm{P}\Gamma\mathrm{L}_n(q)$ where $q = p^f$

For the remainder of this section let $Z = Z(\mathrm{GL}_n(F))$. This is the set of all non-zero scalar multiples of the identity matrix, and this is isomorphic to $F^\times$, the multiplicative group of F. Then we may form the following quotient groups.

Definition 2.2.17. The *projective general linear group* is

$$\mathrm{PGL}_n(F) = \mathrm{GL}_n(F)/Z.$$

This generalises to the following.

Definition 2.2.18. Let $X \leq \mathrm{GL}_n(F)$. Then the corresponding projective group $X/(X \cap Z)$ is denoted PX or $\bar{X}$.

The groups $\mathrm{PSL}_n(q)$ are usually simple and form one of the infinite families of finite simple groups. We state the order of these groups, for example as given in the Atlas [17].

Proposition 2.2.19. *The order of* $\mathrm{PSL}_n(q)$ *is*

$$\frac{1}{d} q^{n(n-1)/2} \prod_{i=2}^{n} (q^i - 1)$$

where $d = (n, q-1)$.

Then we have the following chains of subgroups

$$\mathrm{SL}_n(q) \leq \mathrm{GL}_n(q) \leq \Gamma\mathrm{L}_n(q) \text{ and } \mathrm{PSL}_n(q) \leq \mathrm{PGL}_n(q) \leq \mathrm{P}\Gamma\mathrm{L}_n(q).$$

The indices of these subgroups are given in [44, Tables 2.1.C & 2.1.D] and reproduced as Table 2.1. Using Propositions 2.2.3 and 2.2.19 we may calculate the orders of all these groups.

Now we move on to some definitions that are required to define the remaining classical groups.

Definition 2.2.20. If σ is an automorphism of a field F, a *σ-sesquilinear form* on $V = F^n$ is a map $\beta : V \times V \to F$ such that

1. $\beta(u_1 + u_2, v) = \beta(u_1, v) + \beta(u_2, v)$,
2. $\beta(u, v_1 + v_2) = \beta(u, v_1) + \beta(u, v_2)$,

3. $\beta(au, bv) = a\beta(u, v)b^\sigma$

for all $u, u_1, u_2, v, v_1, v_2 \in V$, $a, b \in F$.

Definition 2.2.21. Let β be a σ-sesquilinear form as described above.

- If $\sigma = 1$, the form is *bilinear*.
- A sesquilinear form β such that $\beta(u, v) = 0$ implies $\beta(v, u) = 0$ for all $u, v \in V$, is said to be *reflexive*.

Now suppose β is reflexive.

- A form β is *non-degenerate* if $\beta(u, v) = 0$ for all $u \in V$ implies $v = 0$.
- A pair of vectors (u, v) such that $\beta(u, v) = 0$ is said to be *orthogonal*.
- For $X \subseteq V$, the set $X^\perp = \{u \in V : \beta(u, v) = 0 \text{ for all } v \in X\}$ is the *orthogonal complement* of X.
- A subspace $W \subseteq V$ is *non-degenerate* if $W \cap W^\perp = \{0\}$.
- If $V = U \oplus W$ and $\beta(u, w) = 0$ for all $u \in U$, $w \in W$, then V is the *orthogonal direct sum* of U and W and we write $V = U \perp W$.
- A non-zero vector $v \in V$ is *isotropic* if $\beta(v, v) = 0$.
- A subspace W is *totally isotropic* if $W \subseteq W^\perp$.

Note that a reflexive form β is non-degenerate if and only if $V^\perp = \{0\}$. The totally isotropic subspaces are precisely the subspaces on which the form is zero.

Definition 2.2.22. Let $\beta : V \times V \to F$ be a σ-sesquilinear form.

- If β is a bilinear form such that $\beta(v, v) = 0$ for all $v \in V$, then β is *alternating*.
- If β is a bilinear form such that $\beta(u, v) = \beta(v, u)$ for all $u, v \in V$, then β is *symmetric*.
- If $\beta(u, v) = \beta(v, u)^\sigma$ for all $u, v \in V$, and σ has order 2, then β is *Hermitian*.

As we shall see, symplectic, orthogonal and unitary groups are subsets of $\mathrm{GL}(V)$ preserving these forms. The definition of a symmetric bilinear form is not enough to define orthogonal groups, thus we introduce quadratic forms.

Definition 2.2.23. A *quadratic form* on V is a function $Q : V \to \mathbb{F}$ such that

$$Q(\lambda v) = \lambda^2 Q(v)$$

for $\lambda \in \mathbb{F}$, $v \in V$, and

$$\beta(u, v) = Q(u + v) - Q(u) - Q(v)$$

is a bilinear form. We say β is the *polar form* of Q, or that Q *polarises* to β.

Observe that $\beta(v, v) = 2Q(v)$, so when the characteristic of F is not equal to 2, Q is determined by β and vice-versa.

Definition 2.2.24. Let $Q : V \to F$ be a quadratic form. A non-zero vector v is *singular* if $Q(v) = 0$. A subspace $W \leq V$ is *totally singular* if $Q(w) = 0$, for all $w \in W$. If β is an alternating or Hermitian form, a non-zero vector v is *singular* if it is isotropic, and a subspace $W \leq V$ is *totally singular* if it is totally isotropic.

We make the distinction between isotropic and singular as in the orthogonal case there are non-singular vectors which are isotropic.

Definition 2.2.25. Let V be a vector space over a field F equipped with a non-degenerate alternating or Hermitian form β, or a non-degenerate quadratic form Q. Then $g \in \mathrm{GL}_n(F)$ is a *similarity* if there exists a $\lambda \in F$ such that $\beta(v_1 g, v_2 g) = \lambda\beta(v_1, v_2)$ for all $v_1, v_2 \in V$, or $Q(vg) = \lambda Q(v)$ for all $v \in V$.

The conformal groups are the set of all similarities with respect to a suitable form. Now we define the symplectic, unitary and orthogonal groups. As with $\mathrm{GL}_n(q)$, in each case we define the special and semilinear groups, and the corresponding projective groups.

Definition 2.2.26. Let β be an non-degenerate alternating form on a vector space $V = F^n$. The *symplectic group* is

$$\mathrm{Sp}(V) = \{g \in \mathrm{GL}(V) : \beta(ug, vg) = \beta(u, v) \text{ for all } u, v \in V\}.$$

So, the symplectic group is the set of all elements in $\mathrm{GL}(V)$ preserving the alternating form β. It does not matter which non-degenerate alternating form β we choose. By [44, Proposition 2.4.1] the isomorphism type of $\mathrm{Sp}(V)$ is independent of the choice of β and V always has even dimension. Then if $F = \mathbb{F}_q$, we may write $\mathrm{Sp}(V) = \mathrm{Sp}_{2m}(q)$. We state its order (for example, as stated in the Atlas).

Proposition 2.2.27. *The order of* $\mathrm{Sp}_{2m}(q)$ *is*

$$q^{m^2} \prod_{i=1}^{m} (q^{2i} - 1).$$

Groups	Index	Groups	Index
$[\Gamma\mathrm{Sp}_{2m}(q) : \mathrm{CSp}_{2m}(q)]$	f	$[\mathrm{PCSp}_{2m}(q) : \mathrm{PSp}_{2m}(q)]$	$(2, q-1)$
$[\mathrm{CSp}_{2m}(q) : \mathrm{Sp}_{2m}(q)]$	$q-1$	$[\mathrm{P\Gamma Sp}_{2m}(q) : \mathrm{PCSp}_{2m}(q)]$	f

Table 2.2: Indices of subgroups of $\Gamma\mathrm{Sp}_{2m}(q)$ and $\mathrm{P\Gamma Sp}_{2m}(q)$ where $q = p^f$

Definition 2.2.28. Let β be a non-degenerate alternating form on $V = \mathbb{F}_q^{2m}$.

- The *semilinear symplectic group*, $\Gamma\mathrm{Sp}_{2m}(q)$, is the set of $g \in \Gamma\mathrm{L}_{2m}(q)$ such that there exist $\lambda \in \mathbb{F}_q$ and $\sigma \in \mathrm{Aut}(\mathbb{F}_q)$, such that $\beta(ug, vg) = \lambda\beta(u, v)^\sigma$ for all $u, v \in V$.
- The *conformal symplectic group*, $\mathrm{CSp}_{2m}(q)$, is the set of all similarities $g \in \mathrm{GL}_{2m}(q)$ with respect to the form β.

All elements of $\mathrm{Sp}_{2m}(q)$ have determinant 1 ([87, Corollary 8.6]) and so we do not need to define the corresponding special group. We may also define the corresponding projective groups. As we shall see, all but finitely many of these groups are simple. The order of $\mathrm{PSp}_{2m}(q)$ can be found in the Atlas and we state it below.

Proposition 2.2.29. *The order of* $\mathrm{PSp}_{2m}(q)$ *is*

$$\frac{1}{d} q^{m^2} \prod_{i=1}^{m} (q^{2i} - 1)$$

where $d = (2, q-1)$.

Then we have the following chains of subgroups

$$\mathrm{Sp}_{2m}(q) \leq \mathrm{CSp}_{2m}(q) \leq \Gamma\mathrm{Sp}_{2m}(q) \text{ and } \mathrm{PSp}_{2m}(q) \leq \mathrm{PCSp}_{2m}(q) \leq \Gamma\mathrm{Sp}_{2m}(q).$$

As we have orders of $\mathrm{Sp}_{2m}(q)$ and $\mathrm{PSp}_{2m}(q)$, we display the indices of the remaining subgroups in Table 2.2 (from [44, Tables 2.1.C & 2.1.D]) allowing us to obtain the orders of any of these groups.

Definition 2.2.30. Let β be a non-degenerate σ-Hermitian form on a vector space $V = F^d$, where σ is an automorphism of F of order 2. The *unitary group* is

$$\mathrm{GU}(V) = \{g \in \mathrm{GL}(V) : \beta(ug, vg) = \beta(u, v) \text{ for all } u, v \in V\}.$$

Up to isomorphism there is one unitary group of each dimension over each finite field F. It can be shown that $F = \mathbb{F}_{q^2}$ for some prime power q. If $V = \mathbb{F}_{q^2}$, we denote $\mathrm{GU}(V) \leq \mathrm{GL}_n(q^2)$ by $\mathrm{GU}_n(q)$. We state the order of these groups here (as stated in the Atlas).

Groups	Index
$[\mathrm{GU}_n(q) : \mathrm{SU}_n(q)]$	$q+1$
$[\mathrm{CGU}_n(q) : \mathrm{GU}_n(q)]$	$q-1$
$[\Gamma\mathrm{U}_n(q) : \mathrm{CGU}_n(q)]$	$2f$

Groups	Index
$[\mathrm{PGU}_n(q) : \mathrm{PSU}_n(q)]$	$(n, q+1)$
$[\mathrm{PCGU}_n(q) : \mathrm{PGU}_n(q)]$	1
$[\mathrm{P\Gamma U}_n(q) : \mathrm{PCGU}_n(q)]$	$2f$

Table 2.3: Indices of subgroups of $\Gamma\mathrm{U}_n(q)$ and $\mathrm{P\Gamma U}_n(q)$ where $q = p^f$

Proposition 2.2.31. *The order of* $\mathrm{GU}_n(q)$ *is*

$$q^{n(n-1)/2} \prod_{i=1}^{n} (q^i - (-1)^i).$$

Definition 2.2.32. Let $V = \mathbb{F}_{q^2}^n$, a vector space equipped with a non-degenerate Hermitian form β. Then we define the following.

- The *semilinear unitary group* is the set of $g \in \Gamma\mathrm{L}_n(q^2)$ such that there exists $\lambda \in \mathbb{F}_{q^2}^\times$ and $\sigma \in \mathrm{Aut}(\mathbb{F}_q^2)$ such that $\beta(ug, vg) = \lambda\beta(u, v)^\sigma$ for all $u, v \in V$.
- The *conformal unitary group*, $\mathrm{CGU}_n(q)$, is the set of similarities in $\mathrm{GL}_n(q^2)$ with respect to the form β.
- The *special unitary group* is $\mathrm{SU}_n(q) = \mathrm{SL}_n(q^2) \cap \mathrm{GU}_n(q)$.

We may also define the corresponding projective groups. Once again the projective special groups are usually simple. The order of $\mathrm{PSU}_n(q)$ is given in the Atlas and we state it here.

Proposition 2.2.33. *The order of* $\mathrm{PSU}_n(q)$ *is*

$$\frac{1}{d} q^{n(n-1)/2} \prod_{i=2}^{n} (q^i - (-1)^i)$$

where $d = (n, q+1)$.

Then we have the following chains of groups

$$\mathrm{SU}_n(q) \leq \mathrm{GU}_n(q) \leq \mathrm{CGU}_n(q) \leq \Gamma\mathrm{U}_n(q)$$

and

$$\mathrm{PSU}_n(q) \leq \mathrm{PGU}_n(q) \leq \mathrm{CGU}_n(q) \leq \mathrm{P\Gamma U}_n(q).$$

The indices of these subgroups are given in [44, Tables 2.1.C & 2.1.D], and the appropriate information is displayed in Table 2.3. Combined with Propositions 2.2.31 and 2.2.33, we may obtain the order of any of these subgroups.

Finally we define the orthogonal groups.

Definition 2.2.34. Let Q be a non-degenerate quadratic form $Q : V \to F$ whose polar form is $\beta(u, v) = Q(u+v) - Q(u) - Q(v)$. The *orthogonal group* associated with V and Q is

$$\mathrm{GO}(V, Q) = \{g \in \mathrm{GL}(V) : Q(vg) = Q(v) \text{ for all } v \in V\}.$$

The group may be denoted $\mathrm{GO}(V)$ if the quadratic form is clear. If the dimension of V is odd, then there is one such subgroup up to isomorphism. If the dimension of V is even, then there are two such subgroups referred to as *plus type* and *minus type*. These groups are denoted $\mathrm{GO}_n^\epsilon(q)$ where ϵ is $\circ$, $+1$, or -1 accordingly. When n is odd, the group $\mathrm{GO}_n^\circ(G)$ may be denoted $\mathrm{GO}_n(q)$.

Theorem 2.2.35 ([87, Theorem 11.9])**.** *$\mathrm{GO}_{2m+1}(2^k)$ is isomorphic to $\mathrm{Sp}_{2m}(2^k)$.*

Henceforth we assume that if we have an orthogonal group of odd dimension that it is over a field of odd characteristic. The order of these groups is as follows.

Proposition 2.2.36. *The order of $\mathrm{GO}_{2m+1}^\circ(q)$ is*

$$2q^{m^2} \prod_{i=1}^{m} (q^{2i} - 1).$$

The order of $\mathrm{GO}_{2m}^\pm(q)$ is

$$2q^{m(m-1)}(q^m \mp 1) \prod_{i=1}^{m-1} (q^{2i} - 1).$$

Definition 2.2.37. Let $V = \mathbb{F}_q^n$ be a vector space equipped with a non-degenerate quadratic form Q, and let ϵ be one of $-$, $\circ$, $+$. Then we define the following.

- The *semilinear orthogonal group*, denoted $\Gamma\mathrm{O}_n^\epsilon(q)$, is the set of $g \in \Gamma\mathrm{L}_n(q)$ such that there exists $\lambda \in \mathbb{F}_q^\times$ and $\sigma \in \mathrm{Aut}(\mathbb{F}_q)$, such that $Q(vg) = \lambda Q(v)^\sigma$ for all $v \in V$.
- The *special orthogonal group* is $\mathrm{SO}_n^\epsilon(q) = \mathrm{SL}_n(q) \cap \mathrm{GO}_n^\epsilon(q)$.
- The *conformal orthogonal group* $\mathrm{CGO}_n^\epsilon(q)$, is the set of all similarities in $\mathrm{GL}_n(q)$ with respect to the quadratic form Q.

We shall be interested in a particular subgroup of $\mathrm{GO}_n^\epsilon(q)$, as the corresponding projective group is usually simple.

Definition 2.2.38. The derived subgroup $\mathrm{GO}_n^\epsilon(q)'$ of $\mathrm{GO}_n^\epsilon(q)$ is denoted $\Omega_n^\epsilon(q)$.

Groups	Index
$[\mathrm{SO}_{2m+1}(q) : \Omega_{2m+1}(q)]$	2
$[\mathrm{GO}_{2m+1}(q) : \mathrm{SO}_{2m+1}(q)]$	2
$[\mathrm{CGO}_{2m+1}(q) : \mathrm{GO}_{2m+1}(q)]$	$\frac{1}{2}(q-1)$
$[\Gamma\mathrm{O}_{2m+1}(q) : \mathrm{CGO}_{2m+1}(q)]$	f

Table 2.4: Indices of subgroups of $\Gamma\mathrm{O}_{2m+1}(q)$ where $q = p^f$

Groups	Index
$[\mathrm{SO}^{\pm}_{2m}(q) : \Omega^{\pm}_{2m}(q)]$	2
$[\mathrm{GO}^{\pm}_{2m}(q) : \mathrm{SO}^{\pm}_{2m}(q)]$	$(2, q-1)$
$[\mathrm{CGO}^{\pm}_{2m}(q) : \mathrm{GO}^{\pm}_{2m}(q)]$	$(q-1)$
$[\Gamma\mathrm{O}^{\pm}_{2m}(q) : \mathrm{CGO}^{\pm}_{2m}(q)]$	f

Table 2.5: Indices of subgroups of $\Gamma\mathrm{O}^{\pm}_{2m}(q)$ where $q = p^f$

We may also define the corresponding projective groups. If n is odd, then $\mathrm{P}\Omega_n(q) = \Omega_n(q)$.

Proposition 2.2.39. *The order of* $\mathrm{P}\Omega^{\pm}_{2m}(q)$ *is*

$$\frac{1}{d} q^{m(m-1)}(q^m \mp 1) \prod_{i=1}^{m-1} (q^{2i} - 1),$$

where $d = (4, q^m \mp 1)$.

Then we obtain the following chain of subgroups

$$\Omega^{\epsilon}_n(q) \leq \mathrm{SO}^{\epsilon}_n(q) \leq \mathrm{GO}^{\epsilon}_n(q) \leq \mathrm{CGO}^{\epsilon}_n(q) \leq \Gamma\mathrm{O}^{\epsilon}_n(q).$$

If n is even, then

$$\mathrm{P}\Omega^{\pm}_n(q) \leq \mathrm{PSO}^{\pm}_n(q) \leq \mathrm{PGO}^{\pm}_n(q) \leq \mathrm{PCGO}^{\pm}_n(q) \leq \mathrm{P}\Gamma\mathrm{O}^{\pm}_n(q).$$

The indices of these subgroups are given in [44, Tables 2.1.C & 2.1.D], and the appropriate information is reproduced as Tables 2.4, 2.5 and 2.6. Together with Propositions 2.2.36 and 2.2.39, this allows us to calculate the order of any of these subgroups.

Groups	Index
$[\mathrm{PSO}^{\pm}_{2m}(q) : \mathrm{P}\Omega^{\pm}_{2m}(q)]$	$2(2, q-1)/(4, q^m \mp 1)$
$[\mathrm{PGO}^{\pm}_{2m}(q) : \mathrm{PSO}^{\pm}_{2m}(q)]$	$(2, q-1)$
$[\mathrm{PCGO}^{\pm}_{2m}(q) : \mathrm{PGO}^{\pm}_{2m}(q)]$	$(2, q-1)$
$[\mathrm{P}\Gamma\mathrm{O}^{\pm}_{2m}(q) : \mathrm{PCGO}^{\pm}_{2m}(q)]$	f

Table 2.6: Indices of subgroups of $\mathrm{P}\Gamma\mathrm{O}^{\pm}_{2m}(q)$ where $q = p^f$

2.2.2 Simple classical groups & Aschbacher's theorem

Now we concentrate on simple classical groups.

Theorem 2.2.40. *The following are isomorphisms between classical groups.*

1. $\mathrm{PSL}_2(q) \cong \mathrm{PSp}_2(q) \cong \mathrm{PSU}_2(q)$.
2. $\mathrm{PSL}_2(q) \cong \mathrm{P}\Omega_3(q)$ *when* q *is odd.*
3. $\mathrm{PSL}_2(q^2) \cong \Omega_4^-(q)$.
4. $\mathrm{PSp}_4(q) \cong \mathrm{P}\Omega_5(q)$ *when* q *is odd.*
5. $\mathrm{PSL}_4(q) \cong \mathrm{P}\Omega_6^+(q)$.
6. $\mathrm{PSU}_4(q) \cong \mathrm{P}\Omega_6^-(q)$.
7. $\mathrm{PSL}_2(7) \cong \mathrm{PSL}_3(2)$.
8. $\mathrm{PSL}_2(4) \cong \mathrm{PSL}_2(5)$.
9. $\mathrm{PSL}_2(9) \cong \mathrm{Sp}_4(2)'$.

Proof. See [44, Proposition 2.9.1]. □

There are also isomorphisms between alternating and classical groups: $A_5 \cong \mathrm{PSL}_2(5)$, $A_6 \cong \mathrm{PSL}_2(9)$, $A_8 \cong \mathrm{PSL}_4(2)$. In light of these isomorphisms we may assume that if we are considering a symplectic group the dimension is greater than or equal to 4 (symplectic groups always have even dimension), if we are considering a unitary group the dimension is at least 3 and if we are considering an orthogonal group the dimension is at least 7. We also assume whenever we have an orthogonal group of odd dimension over $\mathbb{F}_q$, that q is also odd.

Then by [44, Theorem 2.1.3] we may list all the simple classical groups.

Theorem 2.2.41. *Let* G *be a simple classical group. Then* G *is isomorphic to one of the groups listed below.*

1. $\mathrm{PSL}_n(q)$ *for* $n \geq 2$*, and excluding* $\mathrm{PSL}_2(2)$ *and* $\mathrm{PSL}_2(3)$.
2. $\mathrm{PSp}_{2m}(q)$ *for* $m \geq 2$*, and excluding* $\mathrm{PSp}_4(2)$.
3. $\mathrm{PSU}_n(q)$ *for* $n \geq 3$ *except for* $\mathrm{PSU}_3(2)$.
4. $\Omega_n(q)$ *for* $n \geq 7$*,* n *and* q *both odd.*
5. $\mathrm{P}\Omega_n^{\pm}(q)$ *for* $n \geq 8$.

Conversely, all these groups listed are simple.

G	$\rho(G)$
$\mathrm{PSL}_n(q)$	$(q^n-1)/(q-1)$
$(n,q) \neq (2,5),(2,7),$	
$(2,9),(2,11),(4,2)$	
$\mathrm{PSL}_2(5)$, $\mathrm{PSL}_2(7)$, $\mathrm{PSL}_2(9)$	5, 7, 6
$\mathrm{PSL}_2(11)$, $\mathrm{PSL}_4(2)$	11, 8
$\mathrm{PSp}_{2m}(q)$, $m \geq 2$, $q > 2$	$(q^{2m}-1)/(q-1)$
$(m,q) \neq (2,3)$	
$\mathrm{Sp}_{2m}(2)$, $m \geq 3$	$2^{m-1}(2^m-1)$
$\mathrm{Sp}_4(2)'$, $\mathrm{PSp}_4(3)$	6, 27
$\mathrm{PSU}_3(q)$, $q \neq 2,5$	q^3+1
$\mathrm{PSU}_3(5)$	50
$\mathrm{PSU}_4(q)$	q^4+q^3+q+1
$\mathrm{PSU}_n(q)$, $n \geq 5$,	$(q^n-(-1)^n)(q^{n-1}-(-1)^{n-1})/(q^2-1)$
$(n,q) \neq (2m,2)$	
$\mathrm{PSU}_n(2)$, n even, $n \geq 6$	$2^{n-1}(2^n-1)/3$
$\Omega_{2m+1}(q)$, $m \geq 3$, $q \geq 5$ odd	$(q^{2m}-1)/(q-1)$
$\Omega_{2m+1}(3)$, $m \geq 3$	$3^m(3^m-1)/2$
$\mathrm{P}\Omega^+_{2m}(q)$, $m \geq 4$, $q \geq 4$	$(q^m-1)(q^{m-1}+1)/(q-1)$
$\mathrm{P}\Omega^+_{2m}(2)$, $m \geq 4$	$2^{m-1}(2^m-1)$
$\mathrm{P}\Omega^+_{2m}(3)$, $m \geq 4$	$3^{m-1}(3^m-1)/2$
$\mathrm{P}\Omega^-_{2m}(q)$, $m \geq 4$	$(q^m+1)(q^{m-1}-1)/(q-1)$

Table 2.7: Smallest degree of permutation representations of simple classical groups G

Alternative notation for these groups (as in the ATLAS [17]) is $\mathrm{L}_n(q) = \mathrm{PSL}_n(q)$, $\mathrm{S}_n(q) = \mathrm{PSp}_n(q)$, $\mathrm{U}_n(q) = \mathrm{PSU}_n(q)$, $\mathrm{O}_n(q) = \Omega_n(q)$, $\mathrm{O}^{\pm}_n(q) = \mathrm{P}\Omega^{\pm}_n(q)$. Additionally, each of these families of classical groups can be considered as one of the families of groups of Lie type. This will be discussed in Section 2.3.

Minimal degrees of permutation representations of simple classical groups are used throughout, and so we state them here. These degrees are given by the following theorem (corrections in [44, Theorem 5.2.2] and [9]).

Theorem 2.2.42 ([18])**.** *Let $\rho(G)$ denote the smallest degree of a non-trivial permutation representation of a simple classical group G. Then $\rho(G)$ is given in Table 2.7.*

Let Γ be a semilinear group, let $\bar{\Gamma}$ denote the corresponding projective group, and let $\bar{\Omega}$ denote the corresponding simple group. When $\Gamma = \Gamma\mathrm{L}_n(q)$ for $n \geq 3$, then $\mathrm{SL}_n(q)$ possesses an inverse-transpose automorphism ι. Then in this case define $A = \Gamma : \langle \iota \rangle$, for all other Γ, let $A = \Gamma$. Let $\bar{A}$ denote the corresponding projective group. In most cases $\bar{A} = \mathrm{Aut}(\bar{\Omega})$ as described in the following theorem.

Theorem 2.2.43 ([44, Theorem 2.1.4])**.** *Let $\bar{\Omega}$ be a simple classical group where $n \geq 2$ if $\bar{\Omega} = \mathrm{PSL}_n(q)$, $n \geq 3$ if $\bar{\Omega} = \mathrm{PSU}_n(q)$, $n \geq 4$ if $\bar{\Omega} = \mathrm{PSp}_n(q)$, and $n \geq 7$ if $\bar{\Omega} = \mathrm{P}\Omega^{\epsilon}_n(q)$. Then $\bar{A} = \mathrm{Aut}(\bar{\Omega})$ except when $\Omega = \mathrm{Sp}_4(q)$ with q even and when $\Omega = \Omega^+_8(q)$.*

In these cases where $\bar{A} \neq \mathrm{Aut}(\bar{\Omega})$, the automorphisms in $\mathrm{Aut}(\bar{\Omega}) \setminus \bar{A}$ are graph automorphisms. These will be given in the next section, when we discuss groups of Lie type.

By Aschbacher's theorem [2], maximal subgroups of classical groups fall into one of 9 classes, $\mathcal{C}_1$ to $\mathcal{C}_8$ and $\mathcal{S}$ (or $\mathcal{C}_9$). For the rest of this section let $G_0 \leq G \leq \mathrm{Aut}(G_0)$ where G_0 is a simple group of the form $\mathrm{PSL}_n(q)$, $\mathrm{PSp}_n(q)$, $\mathrm{PSU}_n(q)$ or $\mathrm{P}\Omega^{\epsilon}_n(q)$. Let V denote the natural n-dimensional module over the field F associated with G. So if $G_0 = \mathrm{PSU}_n(q)$ then $F = \mathbb{F}_{q^2}$, and $F = \mathbb{F}_q$ otherwise. A brief description of the classes $\mathcal{C}_1$ to $\mathcal{C}_8$ of maximal subgroups (as in [44, Table 1.2.A]) is as follows.

$\mathcal{C}_1$: Stabilisers of totally singular or non-degenerate subspaces of V.
$\mathcal{C}_2$: Stabilisers of direct sum decompositions of $V = \bigoplus_{i=1}^{t} V_i$.
$\mathcal{C}_3$: Stabilisers of extension fields of $\mathbb{F}_q$ of prime index.
$\mathcal{C}_4$: Stabilisers of tensor product decompositions $V = V_1 \otimes V_2$, where V_1 and V_2 are of different dimensions.
$\mathcal{C}_5$: Stabilisers of subfields of $\mathbb{F}_q$ of prime index.
$\mathcal{C}_6$: Normalisers of symplectic-type r-groups ($r \neq p$ prime) in absolutely irreducible representations.
$\mathcal{C}_7$: Stabilisers of tensor product decompositions $V = \bigotimes_{i=1}^{t} V_i$ with each V_i of the same dimension.
$\mathcal{C}_8$: Classical subgroups.

Definition 2.2.44. We refer to the maximal subgroups of G in classes $\mathcal{C}_1$ to $\mathcal{C}_8$ as *geometric maximal subgroups*, and we denote the set of such subgroups by $\mathcal{C}_G$.

Definition 2.2.45. A subgroup H of G lies in $\mathcal{S}$ if and only if the following hold.

1. The socle S of H is a non-abelian simple group.
2. If L is the full covering group of S, and if $\rho : L \to \mathrm{GL}(V)$ is a representation of L such that $L\rho/(Z(\mathrm{GL}(V)) \cap L) = S$, then ρ is absolutely irreducible.
3. $L\rho$ cannot be realised over a proper subfield of F.
4. If $L\rho$ fixes a non-degenerate quadratic form on V, then $G_0 = \mathrm{P}\Omega^{\epsilon}_n(q)$.
5. If $L\rho$ fixes a non-degenerate symplectic form on V, but does not fix a non-degenerate quadratic form, then $G_0 = \mathrm{PSp}_n(q)$.

6. If $L\rho$ fixes a non-degenerate unitary form on V, then $G_0 = \mathrm{PSU}_n(q)$.

2.3 Finite simple groups

The classification of finite simple groups is as follows.

Theorem 2.3.1 (Classification theorem for finite simple groups)**.** *Every finite simple group is isomorphic to one of the following.*

1. *A cyclic group C_p of prime order.*
2. *An alternating group A_n of degree at least 5.*
3. *A simple group of Lie type.*
4. *One of 26 sporadic simple groups.*

The proof of this is spread throughout hundreds of papers. We shall use this result throughout this thesis. The orders of the finite simple groups are known (for example in the Atlas [17]), and it is a consequence of the classification of finite simple groups that there are at most 2 non-abelian finite simple groups of any order $k \in \mathbb{N}$. The Feit–Thompson theorem [26] tells us that all non-abelian simple groups have even order. So, for any $k \in \mathbb{N}$, there are at most k non-abelian simple groups of order at most k.

The alternating groups A_n are simple for $n \geq 5$. If $n \neq 6$, $\mathrm{Aut}(A_n) = S_n$, when $n = 6$, $\mathrm{Aut}(A_6) = S_6 \rtimes C_2$. Note that $A_6 \cong \mathrm{PSL}_2(9)$, and considered as a classical group, the outer automorphism group has the expected order. The smallest non-abelian simple group is $A_5 \cong \mathrm{PSL}_2(4) \cong \mathrm{PSL}_2(5)$ which has order 60. More information about permutation groups is given above in Section 2.1.

Groups of Lie type are either classical groups or exceptional groups. Classical groups have been described in the previous section. We shall give a brief introduction to groups of Lie type, concentrating on the exceptional groups.

Simple Lie algebras are parametrised by Dynkin diagrams which are labelled A_n, B_n, C_n, D_n, E_6, E_7, E_8, F_4 or G_2. These are displayed in Figure 2.1. The subscripts denote the number of nodes in the Dynkin diagram. For each of these we get a corresponding family of groups of Lie type which can be defined over finite fields $\mathbb{F}_q$. These are the untwisted groups of Lie type and fall into the following families: $\mathrm{A}_n(q)$, $\mathrm{B}_n(q)$, $\mathrm{C}_n(q)$, $\mathrm{D}_n(q)$, $\mathrm{E}_6(q)$, $\mathrm{E}_7(q)$, $\mathrm{E}_8(q)$, $\mathrm{F}_4(q)$ and $\mathrm{G}_2(q)$. Symmetries of the Dynkin diagrams yield automorphisms (called graph automorphisms) of the groups of Lie type. Elements of the groups $\mathrm{A}_n(q^2)$, $\mathrm{D}_n(q^2)$, $\mathrm{D}_4(q^3)$ and $\mathrm{E}_6(q^2)$ which are fixed by particular automorphisms give us the twisted groups ${}^2\mathrm{A}_n(q)$, ${}^2\mathrm{D}_n(q)$, ${}^3\mathrm{D}_4(q)$ and ${}^2\mathrm{E}_6(q)$. Other automorphisms only occur over particular fields and give the remaining twisted groups: ${}^2\mathrm{B}_2(2^{2m+1}) \leq \mathrm{B}_2(2^{2m+1})$, ${}^2\mathrm{G}_2(3^{2m+1}) \leq$

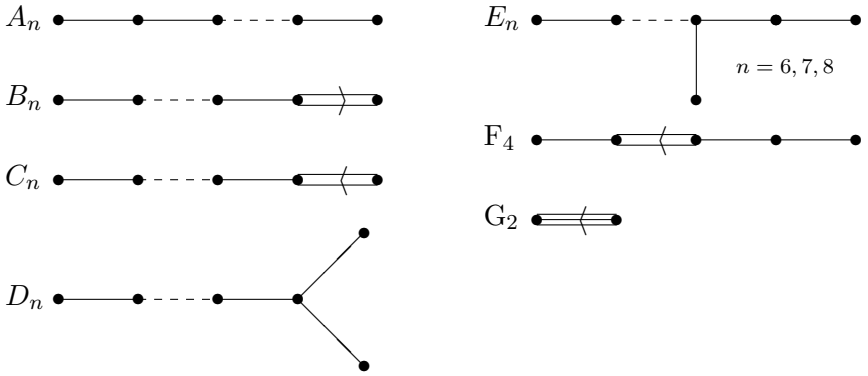


Figure 2.1: Dynkin diagrams

$\mathrm{G}_2(3^{2m+1})$ and ${}^2\mathrm{F}_4(2^{2m+1}) \leq \mathrm{F}_4(2^{2m+1})$. Then the groups of Lie type are the 16 families of untwisted and twisted groups listed above. The groups ${}^2\mathrm{G}_2(q)$, and ${}^2\mathrm{F}_4(q)$ are the Ree groups, and the groups ${}^2\mathrm{B}_2(q)$ are the Suzuki groups, often denoted $\mathrm{Sz}(q)$.

Each group of Lie type has an associated Lie rank, for the untwisted groups this is just the number of nodes in the Dynkin diagram. The twisted Lie groups have both a Lie rank and an untwisted Lie rank. The untwisted Lie rank of a twisted group is the Lie rank of the corresponding untwisted group. The untwisted Lie rank of G shall be denoted $\mathrm{rk}(G)$.

There is a parabolic subgroup associated to every proper subset of the nodes in the Dynkin diagram, and it follows that the maximal parabolic subgroups are those associated to the sets containing all but one of the nodes. In the case where G is classical, parabolic subgroups are stabilisers of totally singular subspaces. If G is a group of Lie type over a field $\mathbb{F}_q$, an (untwisted or twisted) subgroup of the same type as G which is defined over a subfield of $\mathbb{F}_q$ is a subfield or twisted subgroup of G.

The following groups of Lie type are classical groups:

$$\begin{aligned}
&\mathrm{A}_n(q) = \mathrm{PSL}_{n+1}(q),\\
&{}^2\mathrm{A}_n(q) = \mathrm{PSU}_{n+1}(q),\\
&\mathrm{B}_n(q) = \Omega_{2n+1}(q),\\
&\mathrm{C}_n(q) = \mathrm{PSp}_{2n}(q),\\
&\mathrm{D}_n(q) = \mathrm{P}\Omega^+_{2n}(q),\\
&{}^2\mathrm{D}_n(q) = \mathrm{P}\Omega^-_{2n}(q).
\end{aligned}$$

The remaining groups of Lie type are the exceptional groups. The exceptional groups are simple except for:

$$\begin{aligned}
&{}^2\mathrm{B}_2(2) \cong 5:4,\\
&\mathrm{G}_2(2) \cong \mathrm{PSU}_3(3).2,\\
&{}^2\mathrm{G}_2(3) \cong \mathrm{PSL}_2(8).3,\\
&{}^2\mathrm{F}_4(2) = {}^2\mathrm{F}_4(2)'.2.
\end{aligned}$$

Group	Order
$\mathrm{G}_2(q)$	$q^6(q^2-1)(q^6-1)$
$\mathrm{F}_4(q)$	$q^{24}(q^2-1)(q^6-1)(q^8-1)(q^{12}-1)$
$\mathrm{E}_6(q)$	$\frac{1}{d}q^{36}\prod_{i\in\{2,5,6,8,9,12\}}(q^i-1)$
$\mathrm{E}_7(q)$	$\frac{1}{d}q^{63}\prod_{i\in\{2,6,8,10,12,14,18\}}(q^i-1)$
$\mathrm{E}_8(q)$	$q^{120}\prod_{i\in\{2,8,12,14,18,20,24,30\}}(q^i-1)$
${}^2\mathrm{B}_2(q)$	$q^2(q^2+1)(q-1)$
${}^2\mathrm{G}_2(q)$	$q^3(q^3+1)(1-1)$
${}^2\mathrm{F}_4(q)$	$q^{12}(q^6+1)(q^4-1)(q^3+1)(q-1)$
${}^3\mathrm{D}_4(q)$	$q^{12}(q^8+q^4+1)(q^6-1)(q^2-1)$
${}^2\mathrm{E}_6(q)$	$\frac{1}{d}q^{36}\prod_{i\in\{2,5,6,8,9,12\}}(q^i-(-1)^i)$

Table 2.8: Orders of exceptional groups

Whilst ${}^2\mathrm{F}_4(2)$ is not simple, the derived subgroup ${}^2\mathrm{F}_4(2)'$ is, and this subgroup is also known as the Tits group. The Tits group is sometimes considered to be a sporadic group.

The outer automorphism groups of groups of Lie type are made up of diagonal automorphisms, field automorphisms and graph automorphisms. The subgroup of diagonal automorphisms has order d, the subgroup of field automorphisms has order f, the subgroup of graph automorphisms (modulo field automorphisms) has order g, and the outer automorphism group has order dfg. Except when considering outer automorphism groups of $\mathrm{D}_4(q)$, the groups of orders d, f, g, are cyclic or direct products of cyclic groups. Tables 2.8 and 2.9 summarise some information from the Atlas about groups of Lie type.

The sporadic groups are the 26 (or 27 including the Tits group) simple groups that do not lie in one of the other families. The largest of these is the Monster, often denoted M. The groups are as follows: M_{11}, M_{12}, M_{22}, M_{23}, M_{24}, J_2, Suz, HS, McL, Co_1, Co_2, Co_3, He, Fi_{22}, Fi_{23}, Fi'_{24}, HN, Th, B, M, J_1, O′N, J_3, Ly, Ru, J_4. More detail on these groups is given in the Atlas [17]. All the sporadic groups have outer automorphism groups of order one or two.

We will use the following estimate on the order of the outer automorphism group of a non-abelian simple group throughout. Often we just take $|\mathrm{Out}(T)| \leq \log|T|$.

Lemma 2.3.2. *Let T be a non-abelian simple group. Then $|\mathrm{Out}(T)| \leq (6/7)\log|T|$.*

Proof. By the classification of finite simple groups, a non-abelian simple group is either an alternating group A_n, one of 26 sporadic groups, or a group of Lie type. If $T = A_n$ then if $n \neq 6$, $|\mathrm{Out}(T)| = 2$ and if $n = 6$, $|\mathrm{Out}(T)| = 4$. If T is sporadic, $|\mathrm{Out}(T)| = 1$ or 2. In these cases it is clear

Group	d	f	g
$\mathrm{A}_1(q)$	$(2, q-1)$	$q = p^f$	1
$\mathrm{A}_n(q)$, $n \geq 2$	$(n+1, q-1)$	$q = p^f$	2
${}^2\mathrm{A}_n(q)$, $n \geq 2$	$(n+1, q+1)$	$q^2 = p^f$	1
$\mathrm{B}_2(q)$	$(2, q-1)$	$q = p^f$	2 if $p = 2$
			1 otherwise
${}^2\mathrm{B}_2(q)$, f odd	1	$q = 2^f$	1
$\mathrm{B}_n(q)$, $n \geq 3$	$(2, q-1)$	$q = p^f$	1
$\mathrm{C}_n(q)$, $n \geq 3$	$(2, q-1)$	$q = p^f$	1
$\mathrm{D}_4(q)$	$(2, q-1)^2$	$q = p^f$	S_3
${}^3\mathrm{D}_4(q)$	1	$q^3 = p^f$	1
$\mathrm{D}_n(q)$, $n > 4$ even	$(2, q-1)^2$	$q = p^f$	2
$\mathrm{D}_n(q)$, $n > 4$ odd	$(4, q^n - 1)$	$q = p^f$	2
${}^2\mathrm{D}_n(q)$, $n \geq 4$	$(4, q^n + 1)$	$q^2 = p^f$	1
$\mathrm{G}_2(q)$	1	$q = p^f$	2 if $p = 3$
			1 otherwise
${}^2\mathrm{G}_2(q)$, f odd	1	$q = 3^f$	1
$\mathrm{F}_4(q)$	1	$q = p^f$	2 if $p = 2$
			1 otherwise
${}^2\mathrm{F}_4(q)$, f odd	1	$q = 2^f$	1
$\mathrm{E}_6(q)$	$(3, q-1)$	$q = p^f$	2
${}^2\mathrm{E}_6(q)$	$(3, q+1)$	$q^2 = p^f$	1
$\mathrm{E}_7(q)$	$(2, q-1)$	$q = p^f$	1
$\mathrm{E}_8(q)$	1	$q = p^f$	1

Table 2.9: Outer automorphisms of groups of Lie type

T	$\lvert T\rvert \geq$	$\lvert\mathrm{Out}(T)\rvert \leq$
$\mathrm{PSL}_2(q)$, q odd	q^2	$2\log_3 q$
$\mathrm{PSL}_2(q)$, $q \geq 8$ even	$7q^2$	$\log q$
$\mathrm{PSL}_3(q)$	q^7	$6\log q$
$\mathrm{PSL}_n(q)$, $n \geq 4$	q^{3n}	$2n\log q$
$\mathrm{PSp}_n(q)$, $n \geq 4$	q^8	$2\log q$
$\mathrm{PSU}_3(q)$	q^7	$6\log q$
$\mathrm{PSU}_n(q)$, $n \geq 4$	q^{n^2-3}	$2n\log q$
$\Omega_n(q)$, $n \geq 7$ odd	q^{18}	$2\log q$
$\mathrm{P}\Omega_n^{\pm}(q)$, $n \geq 8$ even	q^{24}	$16\log q$
${}^2\mathrm{B}_2(q)$	q^4	$\log q$
$\mathrm{G}_2(q)$	q^6	$\log q$
T exceptional	q^{12}	$6\log q$
$T \neq {}^2\mathrm{B}_2(q)$ or $\mathrm{G}_2(q)$		

Table 2.10: Bounds on orders of $\mathrm{Out}(T)$ for groups of Lie type T

that the bound holds. In all these cases $|T| \geq 60$, and $|\mathrm{Out}(T)| \leq 4$, and we see that $|\mathrm{Out}(T)| \leq (1/2)\log|T|$.

If T is a group of Lie type, then its outer automorphism group has order dfg. The values d, f and g, together with the orders of groups of Lie type, may be found in Section 2.2.1, and Tables 2.8 and 2.9. We list all groups of Lie type T, together with lower bounds on $|T|$, and upper bounds on $|\mathrm{Out}(T)|$ in Table 2.10. From these values it is clear that $|\mathrm{Out}(T)| \leq (6/7)\log|T|$. □

This bound is asymptotically optimal. Consider $T = \mathrm{PSL}_2(2^i)$. Then $|T| = 2^i(2^{2i}-1)$, $\log|T| \simeq 3i$, $|\mathrm{Out}(T)| = i$ and so $|\mathrm{Out}(T)| \simeq (1/3)\log|T|$. When $T = \mathrm{PSL}_3(4)$, $|\mathrm{Out}(T)| = 12$ and $|\mathrm{Out}(T)| = 0.84\log|T| \leq (6/7)\log|T|$.

We have an alternative bound on $|\mathrm{Out}(T)|$ in terms of the degree of a permutation representation of T.

Lemma 2.3.3 ([38, Lemma 2.6])**.** *Let T be a simple group and let $\rho(T)$ be the minimal degree of a faithful transitive permutation representation of T. Then $|\mathrm{Out}(T)| \leq \rho(T)$ and $|\mathrm{Out}(T)| \leq 3\log\rho(T)$.*

Note that any non-trivial permutation representation of a simple group T must be faithful as the kernel of the representation is a normal subgroup of T. A permutation representation of a simple group of minimal degree must be transitive (otherwise T would act transitively on one of the orbits, which would have strictly smaller degree). So if $T \leq S_n$, then $\rho(T) \leq n$.

We will also use the following theorem which tells us when the orders of powers of non-abelian simple groups coincide.

Theorem 2.3.4 ([41, Theorem 6.1])**.** *Let S and T be non-isomorphic finite simple groups. If $|S^a| = |T^b|$ for some natural numbers a and b, then $a = b$ and S and T either are $\mathrm{PSL}_3(4)$ and $\mathrm{PSL}_4(2)$ or are $\Omega_{2n+1}(q)$ and $\mathrm{PSp}_{2n}(q)$ for some $n \geq 3$ and some odd q.*

2.4 Basic estimates

We will use the following definition.

Definition 2.4.1. Let $f(x)$ and $g(x)$ be functions defined on some subset of the real numbers. We write $f(x) = O(g(x))$ if and only if there exists an M, and an x_0, such that $|f(x)| \leq M|g(x)|$ for all $x > x_0$. We say that f is *big-O* of g.

The following basic estimates will be used throughout the thesis.

Lemma 2.4.2. *Let $n \in \mathbb{N}$. Then the following bounds hold.*

- *The number of divisors of n is bounded by $2\sqrt{n}$, and in particular is bounded by n.*
- *The number of prime divisors of n is bounded by $\log n$.*
- *The number of odd prime divisors of n is bounded by $\log_3 n$.*

Proof. Clearly the number of divisors of n is at most n. Let d be a divisor of n. Then either $d = \sqrt{n}$, or precisely one of d and n/d is less than n. Then all divisors of n are of the form d or n/d for some $d \leq \sqrt{n}$. Then the total number of divisors of n is bounded by $2\sqrt{n}$.

Now write $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ where the p_i are distinct primes and $\alpha_i \geq 1$ for $1 \leq i \leq k$. Then $n = p_1^{\alpha_1} \dots p_k^{\alpha_k} \geq 2^{\alpha_1 + \dots + \alpha_k} \geq 2^k$, and so the number of prime divisors $k \leq \log n$. If we are only interested in odd divisors, we are only interested in those $p_i \geq 3$, and the result follows. □

Lemma 2.4.3. *Let $n \in \mathbb{N}$ be fixed, and let $f(x) = (\log x)(\log(n/x))$ for $x \geq 0$. Then this takes its largest value when $x = \sqrt{n}$.*

Proof. We may write

$$f(x) = \log n \log x - (\log x)^2 = \frac{\ln n \ln x}{(\ln 2)^2} - \frac{(\ln x)^2}{(\ln 2)^2}.$$

Then

$$f'(x) = \frac{\ln n - 2 \ln x}{x(\ln 2)^2}.$$

Then $f(x)$ achieves its maximum value when $f'(x) = 0$, that is, precisely when $x = \sqrt{n}$. □

We will also use the following explicit version of Stirling's formula for estimating $n!$ as given in [84, Chapter 8, Question 20],

Lemma 2.4.4. *For $n \in \mathbb{N}$,*

$$n^{n+1/2}e^{-n+7/8} \leq n! \leq n^{n+1/2}e^{-n+1}.$$

Part I

The probability of generating an almost simple group

Chapter 3

The probability of generating an almost simple group

In the first part of this thesis we prove results on the probability of generating almost simple groups with 2 or 3 elements. First we give some basic definitions for probabilistic generation so we can state the main theorem of Part I (Theorem 3.1.7).

3.1 Basic definitions & statement of the main theorems

Definition 3.1.1. Let $d(G)$ denote the minimal number of generators of a group G.

The Euler totient function $\phi(n)$ determines the number of positive integers less than n which are coprime to n. This is precisely the number of elements of the cyclic group C_n that are generators of the group. The following was defined in [32] and generalises this notion.

Definition 3.1.2. The *Eulerian function* $\phi_G(d)$ denotes the number of d-tuples $(g_1, \dots g_d) \in G^d$ such that $\langle g_1, \dots, g_d \rangle = G$.

Definition 3.1.3. If $d \geq d(G)$, define

$$P_G(d) = \frac{\phi_G(d)}{|G|^d},$$

the probability that d independent and uniformly distributed random elements of G generate the group G.

So $P_G(d)$ is the proportion of elements of G^d that generate the group G.

Example 3.1.4. Let $G = C_p$, a cyclic group of prime order p. All elements of G excluding the identity generate the whole group and so the only d-tuple in G^d which does not generate the whole group is $(1, \ldots, 1)$. Then $\phi_G(d) = p^d - 1$ and so $P_G(d) = 1 - 1/p^d$.

We extend this idea as follows.

Definition 3.1.5. Let N be a normal subgroup of a group G, where $d \geq d(G/N)$. Then

$$P_{G,N}(d) = \frac{P_G(d)}{P_{G/N}(d)},$$

the probability that a d-tuple generates G, given that it generates G modulo N.

It follows from the definition that

$$P_{G,N}(d) = \frac{\phi_G(d)}{|N|^d \phi_{G/N}(d)}. \tag{3.1.1}$$

Note that $P_{G,N}(d) = P_G(d)$ when $N = G$.

It is well known that all finite simple groups can be generated by two elements. We have the following result which tells us that almost simple groups can be generated by 3 elements.

Theorem 3.1.6 ([20, Theorem 1])**.** *Let G_0 be a finite non-abelian simple group. If G is an automorphism group of G_0 with $G_0 \leq G \leq \mathrm{Aut}(G_0)$, then $d(G) = \max\{2, d(G/G_0)\}$.*

As $G/G_0 \leq \mathrm{Out}(G_0)$, then $d(G/G_0) \leq 3$ by the Classification of Finite Simple Groups (information about the outer automorphism groups of finite simple groups is given in Section 2.3). It follows that $d(G) \leq 3$ for almost simple groups G.

The outer automorphism groups of groups G_0 of Lie type have order dfg where d, f and g are given in Table 2.9. We see that $d(G) = 3$ implies $G_0 = \mathrm{PSL}_{2m}(p^f)$ for $m \geq 2$, p odd and f even, or $G_0 = \mathrm{P}\Omega^+_{2m}(p^f)$ for $m \geq 4$, p odd and f even.

We are now in a position to state the main theorem of the first part of this thesis.

Theorem 3.1.7. *Let G be an almost simple group with socle G_0 and suppose G can be generated by 2 elements. Then*

$$P_{G,G_0}(2) \geq 53/90 = 0.58\dot{8}$$

with equality if and only if $G = A_6$ or $G = S_6$.

Additionally, $53/90 \leq P_{G,G_0}(2) \leq 8/10$ if and only if G is one of the 8 groups given in Table 3.1, and $8/10 < P_{G,G_0}(2) \leq 9/10$ if and only if G is one of the 22 groups given in Table 3.2.

G	$G_0 = \mathrm{Soc}(G)$	$P_{G,G_0}(2)$	$P_{G,G_0}(2)$
$A_6 \cong \mathrm{PSL}_2(9)$	A_6	53/90	0.588
S_6	A_6	53/90	0.588
$A_5 \cong \mathrm{PSL}_2(4) \cong \mathrm{PSL}_2(5)$	A_5	19/30	0.633
S_5	A_5	19/30	0.633
$\mathrm{PSL}_2(7) \cong \mathrm{PSL}_3(2)$	$\mathrm{PSL}_2(7)$	19/28	0.678
A_7	A_7	229/315	0.726
$A_8 \cong \mathrm{PSL}_4(2)$	A_8	133/180	0.738
$\mathrm{PSL}_2(11)$	$\mathrm{PSL}_2(11)$	127/165	0.769

Table 3.1: Almost simple groups G with $53/90 \leq P_{G,G_0}(2) \leq 8/10$

Proof. By the classification of finite simple groups, G_0 is alternating, classical, exceptional or sporadic, and these cases are considered in Theorems 4.0.1, 5.0.1, 6.0.1 and 7.0.1 respectively. □

Decimal values for the probabilities are rounded down to three decimal places unless otherwise stated. Note that this result shows that if G is a finite simple group then $P_G(2) \geq 53/90$. In addition to the absolute lower bounds given in the theorem we obtain explicit lower bounds on $P_{G,G_0}(2)$ for different families of groups. These bounds are parametrised by n when $G_0 = A_n$; by n and q when G_0 is a classical group of dimension n defined over a field $\mathbb{F}_q$; and by q when G_0 is exceptional group defined over a field $\mathbb{F}_q$. These bounds are given in Chapters 4, 5 and 6 respectively. In most cases we also determine when $P_{G,G_0}(2) \geq 0.927$ which will help us bound the probability for 3-generation.

As all almost simple groups can be generated by 3 elements we also consider $P_{G,G_0}(3)$. The following theorem is proved in Chapter 8.

Theorem 3.1.8. *Let G be an almost simple group with socle G_0. Then $P_{G,G_0}(3) \geq 139/150 = 0.92\dot{6}$, with equality if and only if $G_0 = A_5$.*

The remainder of this chapter proves preliminary lemmas which will give us lower bounds for $P_{G,G_0}(d)$. Using these lemmas, the problem of estimating $P_{G,G_0}(d)$ reduces to estimating the index and number of maximal subgroups of G.

3.2 Lemmas for bounding the probability

We bound the probability in terms of maximal subgroups and we will use the following definition.

Definition 3.2.1. Let G be a normal subgroup of a group $A \leq \mathrm{Aut}(G)$ so that $A = G.K$ for some extension K of G. A maximal subgroup $M < A$ is one of the following types.

G	$G_0 = \mathrm{Soc}(G)$	$P_{G,G_0}(2)$	$P_{G,G_0}(2)$
M_{12}	M_{12}	179/220	0.813
S_8	A_8	4111/5040	0.815
S_7	A_7	103/126	0.817
M_{11}	M_{11}	3239/3960	0.817
$\mathrm{PGL}_2(7)$	$\mathrm{PSL}_2(7)$	23/28	0.821
$\mathrm{PSL}_2(8)$	$\mathrm{PSL}_2(8)$	71/84	0.845
$\mathrm{P\Gamma L}_2(8)$	$\mathrm{PSL}_2(8)$	71/84	0.845
A_9	A_9	15403/18144	0.848
S_9	A_9	78293/90720	0.863
$\mathrm{PSL}_3(3)$	$\mathrm{PSL}_3(3)$	101/117	0.863
$\mathrm{PSL}_3(4)$	$\mathrm{PSL}_3(4)$	121/140	0.864
M_{10}	A_6	13/15	0.866
$\mathrm{PGL}_2(9)$	A_6	13/15	0.866
$A_6.2^2$	A_6	13/15	0.866
A_{10}	A_{10}	29401/33600	0.875
S_{10}	A_{10}	29401/33600	0.875
$\mathrm{PGL}_2(11)$	$\mathrm{PSL}_2(11)$	146/165	0.884
$\mathrm{PSp}_4(3) \cong \mathrm{PSU}_4(2)$	$\mathrm{PSU}_4(2)$	767/864	0.887
$\mathrm{PSU}_4(2).2$	$\mathrm{PSU}_4(2)$	767/864	0.887
A_{11}	A_{11}	743249/831600	0.893
S_{11}	A_{11}	4462987/4989600	0.894
$\mathrm{PSL}_3(4).2_2$	$\mathrm{PSL}_3(4)$	4519/5040	0.896

Table 3.2: Almost simple groups G with $8/10 < P_{G,G_0}(2) \leq 9/10$

1. M is an *ordinary* maximal subgroup if $G \cap M$ is maximal in G.
2. M is a *novelty* maximal subgroup if $G \cap M$ is not maximal in G.
3. M is a *trivial* maximal subgroup if $G \leq M$.

For an almost simple group G with socle G_0 we will be particularly interested in maximal subgroups M of G that do not contain G_0. These are precisely the ordinary and novelty maximal subgroups.

We now prove a result on the probability of generating G with d elements.

Lemma 3.2.2. *Let G be a group that can be generated by d elements, and let $\mathcal{M}$ be a set of conjugacy class representatives for maximal subgroups of G. Then*

$$P_G(d) \geq 1 - \sum_{M <_{\max} G} \frac{1}{[G:M]^d} \geq 1 - \sum_{M \in \mathcal{M}} \frac{1}{[G:M]^{d-1}}.$$

Proof. Let $\Omega = \{(g_1, \ldots, g_d) \in G^d : \langle g_1, \ldots, g_d \rangle = G\}$, that is, the set of d-tuples that generate G. So $|\Omega| = \phi_G(d)$.

If $\langle g_1, \ldots, g_d \rangle \neq G$, then $\langle g_1, \ldots, g_d \rangle \leq M$ for some maximal subgroup M of G. Then

$$\begin{aligned} G^d \setminus \Omega &= \{(g_1, \ldots, g_d) \in G^d : \langle g_1, \ldots, g_d \rangle \neq G\} \\ &= \bigcup_{M <_{\max} G} M^d \end{aligned}$$

and so

$$|G^d \setminus \Omega| \leq \sum_{M <_{\max} G} |M|^d.$$

Then

$$\begin{aligned} \phi_G(d) &= |\Omega| \\ &= |G^d| - |G^d \setminus \Omega| \\ &\geq |G|^d - \sum_{M <_{\max} G} |M|^d, \end{aligned}$$

and so

$$P_G(d) = \frac{\phi_G(d)}{|G|^d} \geq 1 - \sum_{M <_{\max} G} \frac{1}{[G : M]^d}.$$

The number of conjugates of a given maximal subgroup M is equal to $[G : N_G(M)]$. Since $[G : N_G(M)] \leq [G : M]$,

$$\sum_{M <_{\max} G} \frac{1}{[G : M]^d} \leq \sum_{M \in \mathcal{M}} \frac{1}{[G : M]^{d-1}}$$

and the result follows. □

Note that when G is simple, the maximality of M implies $M = N_G(M)$, and so $[G : N_G(M)] = [G : M]$. We may bound $P_{G,N}(d)$ in a similar way. The following will come in useful.

Proposition 3.2.3 ([82, Proposition 2.5.4])**.** *Let G and H be groups such that $d(G) \leq d$. Let $\theta : G \to H$ be an epimorphism and assume that $H = \langle h_1, \ldots, h_d \rangle$. Then there exist $g_1, \ldots, g_d \in G$ such that $G = \langle g_1, \ldots, g_d \rangle$ and $g_i\theta = h_i$ for $1 \leq i \leq d$.*

Proof. For $\mathbf{h} = (h_1, \ldots, h_n) \in H^d$ with $\langle h_1, \ldots, h_d \rangle = H$, let $t_G(\mathbf{h})$ denote the number of d-tuples $\mathbf{g} = (g_1, \ldots, g_d) \in G^d$ such that $\langle g_1, \ldots, g_d \rangle = G$ and $g_i\theta = h_i$ for $1 \leq i \leq d$. We wish to show that $t_G(\mathbf{h}) \geq 1$. Let $\mathbf{g} = (g_1, \ldots, g_d) \in G^d$ such that $g_i\theta = h_i$ for all i and let $K = \ker \theta$. Then any tuple $\mathbf{g}' = (g'_1, \ldots, g'_d)$ with $g'_i\theta = h_i$ for all i, must be in $Kg_1 \times \ldots \times Kg_d$. For $(g_1, \ldots, g_d)$ such that $g_i\theta = h_i$, either $\langle g_1, \ldots, g_d \rangle = G$ or $\langle g_1, \ldots, g_d \rangle = L$ for some proper subgroup $L < G$. Hence

$$t_G(\mathbf{h}) = |K|^d - \sum_{\substack{L < G \\ L\theta = H}} t_L(\mathbf{h}).$$

If $\mathbf{g} = (g_1, \ldots, g_d)$ is a set of generators for G and $h_i = g_i\theta$ for all i, then $t_G(\mathbf{h}) \geq 1$. So if we can show that $t_G(\mathbf{h})$ is independent of the choice of $\mathbf{h}$ then we are done. If G does not contain any proper subgroup L with $L\theta = H$, then $t_G(\mathbf{h}) = |K|^n$ and is therefore independent of choice of $\mathbf{h}$. Then we prove that $t_G(\mathbf{h})$ is independent of $\mathbf{h}$ by induction on $|G|$. We assume that this is true for all epimorphisms $L \to H$ such that $|L| < |G|$. Then it follows that $t_G(\mathbf{h})$ is independent of $\mathbf{h}$. □

If N is a normal subgroup of G, then taking G/N in the previous proposition allows us to prove the following lemma, known as Gaschütz lemma [29] (as stated in [66, Proposition 2.1]). Let θ be the natural homomorphism from G to the factor group G/N. Using the notation of the previous proposition. Let $\mathbf{h} = (Ng_1, \ldots, Ng_d)$ for some $g_1, \ldots, g_d$, where $G/N = \langle Ng_1, \ldots, Ng_d \rangle$. Then $t_G(\mathbf{h})$ is the number of tuples $(g_1n_1, \ldots, g_dn_d) \in G^d$, for $n_i \in N$, where $\langle g_1n_1, \ldots, g_dn_d \rangle = G$. It follows that $t_G(\mathbf{h})$ is the number of d-tuples $(n_1, \ldots n_d) \in N^d$ such that $\langle g_1n_1, \ldots, g_dn_d \rangle = G$. By the proof of the previous proposition, $t_G(\mathbf{h})$ is independent of the choice of $Ng_1, \ldots, Ng_d \in G/N$, equivalently $t_G(\mathbf{h})$ independent of the choice of $g_1, \ldots, g_d \in G$. Then $t_G(\mathbf{h}) = \phi_G(d)/\phi_{G/N}(d)$. Note that $\langle g_1, \ldots, g_d, N \rangle = G$ if and only if $\langle Ng_1, \ldots, Ng_d \rangle = G/N$.

Proposition 3.2.4 ([29])**.** *Let N be a normal subgroup of a group G, and let $g_1, g_2, \ldots, g_d \in G$ be such that $G = \langle g_1, g_2, \ldots, g_d, N \rangle$. If $d(G) \leq d$, then there exist elements $n_1, n_2, \ldots, n_d$ of N such that $G = \langle g_1n_1, \ldots, g_dn_d \rangle$. Moreover, the cardinality of the set $\Omega_{g_1,g_2,\ldots,g_d} = \{(n_1, n_2, \ldots, n_d) \in N^d : \langle g_1n_1, \ldots, g_dn_d \rangle = G\}$ is independent of the choice of $g_1, g_2, \ldots, g_d$, and it is equal to $\phi_G(d)/\phi_{G/N}(d)$.*

The next corollary follows immediately from Equation 3.1.1.

Corollary 3.2.5. *Let G, N and $\Omega_{g_1,g_2,\ldots,g_d}$ be defined as in Proposition 3.2.4. Then*

$$P_{G,N}(d) = \frac{|\Omega_{g_1,g_2,\ldots,g_d}|}{|N|^d}.$$

Similarly to Lemma 3.2.2 we estimate $P_{G,N}(d)$ in terms of the maximal subgroups of G.

Lemma 3.2.6. *Let G be a group that can be generated by d elements, and let N be a normal subgroup of G. Let $\mathcal{M}$ be a set of conjugacy class representatives for maximal subgroups of G that do not contain N. Then*

$$P_{G,N}(d) \geq 1 - \sum_{\substack{M <_{\max} G \\ N \not\leq M}} \frac{1}{[G:M]^d} \geq 1 - \sum_{M \in \mathcal{M}} \frac{1}{[G:M]^{d-1}}.$$

Proof. Fix $g_1, \ldots, g_d \in G$ such that $\langle g_1, g_2, \ldots, g_d, N\rangle = G$. Let

$$\Omega' = \{(n_1, \ldots, n_d) \in N^d : \langle g_1 n_1, \ldots, g_d n_d\rangle \neq G\}.$$

Then by Corollary 3.2.5,

$$P_{G,N}(d) = 1 - \frac{|\Omega'|}{|N|^d}.$$

We estimate Ω' in terms of maximal subgroups M that do not contain N. Note that a d-tuple $(n_1, \ldots, n_d) \in N^d$ satisfies $\langle g_1 n_1, \ldots, g_d n_d\rangle \not\leq G$ if and only if $\langle g_1 n_1, \ldots, g_d n_d\rangle \leq M$ for some maximal subgroup M of G where M does not contain N. If M were to contain both N and $\langle g_1 n_1, \ldots, g_d n_d\rangle$, then $M \geq \langle g_1, \ldots, g_d, N\rangle = G$, a contradiction. Then

$$\Omega' = \bigcup_{\substack{M <_{\max} G \\ N \not\leq M}} \{(n_1, \ldots, n_d) \in N^d : \langle g_1 n_1, \ldots, g_d n_d\rangle \leq M\}.$$

For a maximal subgroup M not containing N, let

$$\begin{aligned} L_M &= \{(n_1, \ldots, n_d) \in N^d : \langle g_1 n_1, \ldots, g_d n_d\rangle \leq M\} \\ &= \{(n_1, \ldots, n_d) \in N^d : g_i n_i \in M \text{ for } 1 \leq i \leq d\}. \end{aligned}$$

As $G = MN$ there exist $k_1, \ldots, k_d \in N$ such that $g_i k_i \in M$ for $1 \leq i \leq d$. Fix such a $k_1, \ldots, k_d$. As $g_i n_i, g_i k_i \in M$, then $(g_i k_i)^{-1}(g_i n_i) = k_i^{-1} n_i \in M$, and so $k_i^{-1} n_i \in M \cap N$. Then $(n_1, \ldots, n_d) \mapsto (k_1^{-1} n_1, \ldots, k_d^{-1} n_d)$ is an injective map from L_M to $(M \cap N)^d$. For $l_i \in M \cap N$, $l_i = k_i^{-1}(k_i l_i)$, and so every $l_i \in M \cap N$ can be expressed as $k_i^{-1} n_i$ for some $n_i \in N$. Consider the set

$$(M \cap N)^d = \{(k_1^{-1} n_1, \ldots, k_d^{-1} n_d) : \text{ for some } n_i \in N\}.$$

Then $g_i k_i \in M$ and $k_i^{-1} n_i \in M$ implies $g_i n_i \in M$ for all $1 \leq i \leq d$. Then for $(k_1^{-1} n_1, \ldots, k_d^{-1} n_d) \in (M \cap N)^d$, there exists $(n_1, n_2, \ldots, n_k) \in L_M$. Then the map from L_M to $(M \cap N)^d$ is a bijection and so $|L_M| = |M \cap N|^d$.

Then

$$\begin{aligned} \Omega' &= \bigcup_{\substack{M <_{\max} G \\ N \not\leq M}} L_M \\ |\Omega'| &\leq \sum_{\substack{M <_{\max} G \\ N \not\leq M}} |M \cap N|^d. \end{aligned}$$

Using the Second Isomorphism Theorem and the maximality of M,

$$M/(M \cap N) \cong MN/N = G/N.$$

It follows that

$$[G : N][N : N \cap M] = [G : M][M : N \cap M] = [G : M][G : N]$$

and so

$$[N : N \cap M] = [G : M].$$

Then

$$\begin{aligned} P_{G,N}(d) &\geq 1 - \sum_{\substack{M <_{\max} G \\ N \not\leq M}} \frac{|N \cap M|^d}{|N|^d} \\ &= 1 - \sum_{\substack{M <_{\max} G \\ N \not\leq M}} \frac{1}{[N : N \cap M]^d} \\ &= 1 - \sum_{\substack{M <_{\max} G \\ N \not\leq M}} \frac{1}{[G : M]^d}. \end{aligned}$$

The number of conjugates of M in G is given by $[G : N_G(M)] \geq [G : M]$ which gives the second inequality. □

We are particularly interested in the case where G is almost simple with socle G_0. Often we have more information about subgroups of G_0, and so we may use the following bounds.

Lemma 3.2.7. *Let G be an almost simple group with socle G_0. Let $\mathcal{M}$ be a set of conjugacy class representatives in G for ordinary and novelty maximal subgroups of G. Let $\mathcal{L}$ be a set of conjugacy class representatives in G_0 for subgroups of the form $M \cap G_0$ for M an ordinary or novelty maximal subgroup of G. Let $\mathcal{K}$ be a set of conjugacy classes in G_0 of subgroups of the form $M \cap G_0$ for M an ordinary or novelty maximal subgroup of any almost simple group with socle G_0. Then the following hold.*

1. *If $M \in \mathcal{M}$ then $[G : M] = [G_0 : M \cap G_0]$.*
2. *If $M \in \mathcal{M}$ then $[G : M] \geq \rho(G_0)$, where $\rho(G_0)$ denotes the smallest degree of a non-trivial permutation representation of G_0.*
3. *For any $d \geq 1$,*

$$\sum_{M \in \mathcal{M}} \frac{1}{[G : M]^d} \leq \sum_{L \in \mathcal{L}} \frac{1}{[G_0 : L]^d} \leq \sum_{K \in \mathcal{K}} \frac{1}{[G_0 : K]^d}.$$

Proof. As $[G : M][M : M \cap G_0] = [G : G_0][G_0 : M \cap G_0]$, then to prove part 1 it suffices to show that $[M : M \cap G_0] = [G : G_0]$. As $G_0 \trianglelefteq G$, the Second Isomorphism Theorem gives $M/(M \cap G_0) \cong MG_0/G_0$. The maximality of

M forces $MG_0 = G$ as required. The minimal index of a subgroup of G_0 is equal to $\rho(G_0)$ and part 2 follows.

For the final part, let $M \in \mathcal{M}$. Then $M \cap G_0$ is conjugate in G_0 to L for some $L \in \mathcal{L}$. Without loss of generality let $M \cap G_0 = L$. As G_0 is normal in G, and M is maximal in G,

$$M/L = M/(M \cap G_0) \cong MG_0/G_0 = G/G_0.$$

It follows that $[G : M] = [G_0 : L]$. The number of conjugates of M in G is equal to the number of conjugates of $L = M \cap G_0$ in G. The conjugacy classes of L in G may split over G_0 giving the first inequality in part 3. As $\mathcal{L} \subseteq \mathcal{K}$ the second inequality in part 3 holds. □

Lemma 3.2.8. *Let H be a normal subgroup of a group G and let M be a subgroup of H. Then the conjugacy class of M in G splits into at most $[G : H]$ conjugacy classes over H.*

Proof. The number of conjugates of M in G is given by $[G : N_G(M)]$, and similarly the number of conjugates of M in H is given by $[H : N_H(M)]$. Then

$$[G : N_H(M)] = [G : H][H : N_H(M)] = [G : N_G(M)][N_G(M) : N_H(M)],$$

that is,

$$[G : H][H : N_H(M)] \geq [G : N_G(M)].$$

So the number of conjugates of M in G is at most $[G : H]$ multiplied by the number of conjugates of M in H, that is, the conjugacy class of M in G splits into at most $[G : H]$ classes over H. □

In particular, suppose M is a subgroup of a simple group G. If there is one such subgroup up to conjugacy in $\mathrm{Aut}(G)$, there are at most $|\mathrm{Out}(G)|$ up to conjugacy in G.

We also have the following lemma which relates subgroups of simple groups to the subgroups of the corresponding quasisimple groups.

Lemma 3.2.9. *Let G be an almost simple group with socle G_0. Let H be a quasisimple group such that $H/Z(H) = G_0$. Let $\mathcal{M}$ be a set of G-conjugacy class representatives for maximal subgroups of G which supplement G_0. Let $\mathcal{L}$ be a set of G_0-conjugacy class representatives for subgroups of the form $M \cap G_0$, where M is a maximal subgroup of G which supplements G_0. Let $\mathcal{L}_0$ be the corresponding subgroups of H, that is, subgroups L of H such that $Z(H) \leq L$ and $L/Z(H) \in \mathcal{L}$. Then*

$$\sum_{M \in \mathcal{M}} \frac{1}{[G : M]} \leq \sum_{L \in \mathcal{L}_0} \frac{1}{[H : L]}.$$

Proof. Let $M \in \mathcal{M}$. Then there exists some $L \in \mathcal{L}_0$ such that $L/Z(H) = M \cap G_0$. Then

$$\begin{aligned}[G : M] &= [MG_0 : G_0] \\ &= [G_0 : M \cap G_0] \\ &= [H : L].\end{aligned}$$

Conjugacy classes of subgroups $M \cap G_0$ in G may split over G_0 giving the inequality. □

Note that the subgroups in $\mathcal{L}_0$ are given up to H-conjugacy. In particular, consider the case where G is an almost simple classical group with socle G_0, and H is the corresponding quasisimple group. Tables in [10] allow us to bound the second sum where H is one of $\mathrm{SL}_n(q)$, $\mathrm{Sp}_n(q)$, $\mathrm{SU}_n(q)$ or $\Omega^\epsilon_n(q)$ and $n \leq 12$. Then this lemma allows us to bound the probability $P_{G,G_0}(2)$ where G is an almost simple classical group of dimension at most 12.

There are situations where the maximal subgroups are not fully known. In the cases we consider, maximal subgroups are of two types. There are subgroups whose order and number up to conjugacy are known, and the remaining subgroups which are almost simple and of bounded order but where the number of such subgroups is unknown. The following lemmas will help us estimate the number and indices of maximal subgroups in the second case. We denote the number of involutions in a group G by $i(G)$. We use the following fact.

Proposition 3.2.10 ([62, Proposition 2.2])**.** *Every finite simple group can be generated by two elements, one of which is an involution.*

This is proved for all simple groups other than $\mathrm{PSU}_3(3)$ in [69], and for $\mathrm{PSU}_3(3)$ in [62]. Then we obtain the following lemma.

Lemma 3.2.11 ([62, Lemma 3.1])**.** *Let $\mathcal{S}(G)$ denote the set of simple subgroups of a group G. Then $\sum_{S \in \mathcal{S}(G)} |S| \leq |G| i(G)$.*

Proof. By Proposition 3.2.10, every $S \in \mathcal{S}(G)$ is generated by two elements, one of which is an involution. Consider all pairs $(x, t) \in G \times G$, where t is an involution, and x is any element of G. The number of such pairs is $|G| i(G)$. If a pair (x, t) generates S, then all pairs (x^s, t^s), $s \in S$, generates S. We may show that all these pairs are distinct. Suppose the pair (x, t) generates S, and suppose $(x^{s_1}, t^{s_1}) = (x^{s_2}, t^{s_2})$ for $s_1, s_2 \in S$. Then $x^{s_1 s_2^{-1}} = x$ and $t^{s_1 s_2^{-1}} = t$. As $S = \langle x, t \rangle$, then $s_1 s_2^{-1} \in Z(S)$. As S is simple this implies $s_1 = s_2$. Then there are $|S|$ distinct pairs (x^s, t^s) for $s \in S$. The result follows. □

Lemma 3.2.12. *Let G be an almost simple group with socle G_0. Let $\mathcal{L}$ be a set of almost simple maximal subgroups of G that do not contain G_0 and let*

$\mathcal{S}$ be the set of socles of maximal subgroups in $\mathcal{L}$. Let m be an upper bound for the order of $M \in \mathcal{L}$, let s be an upper bound on $|\mathrm{Out}(S)|$ for $S \in \mathcal{S}$, and let c be an upper bound on $|\mathrm{Aut}(S)|^{d-1}|\mathrm{Out}(S)|$. Then

1. $\displaystyle\sum_{M\in\mathcal{L}} \frac{1}{[G:M]^d} \leq \frac{i(G_0)m^{d-1}s}{|G_0|^{d-1}}$,

2. $\displaystyle\sum_{M\in\mathcal{L}} \frac{1}{[G:M]^d} \leq \frac{6i(G_0)m^{d-1}\log m}{7|G_0|^{d-1}}$,

3. $\displaystyle\sum_{M\in\mathcal{L}} \frac{1}{[G:M]^d} \leq \frac{i(G_0)c}{|G_0|^{d-1}}$.

Proof. Let $M \in \mathcal{L}$. Then $M = N_G(S)$ for some simple group S, and there is at most one such maximal subgroup M for any simple group $S \leq G$. Then $M \cap G_0 \trianglelefteq M$. As S is the minimal normal subgroup of M, then either $S \leq M \cap G_0$ or $M \cap G_0 = 1$.

Suppose $M \cap G_0 = 1$. As $G_0 \nleq M$ then $G = MG_0$. Then

$$G/G_0 \cong MG_0/G_0 \cong M/M \cap G_0 \cong M.$$

This implies that M is a subgroup of $\mathrm{Out}(G_0)$. By the Schreier Conjecture $\mathrm{Out}(G_0)$ is soluble, but M is insoluble as it is almost simple. Then $M \cap G_0 \neq 1$.

So $S \leq M \cap G_0$ and so it suffices to bound the number of simple subgroups of G_0. We denote the set of simple subgroups of G_0 by $\mathcal{S}(G_0)$. Then

$$\begin{aligned}
\sum_{M\in\mathcal{L}} \frac{1}{[G:M]^d} &\leq \sum_{M\in\mathcal{L}} \frac{|M|^d}{|G_0|^d} \\
&\leq \frac{m^{d-1}}{|G_0|^d} \sum_{M\in\mathcal{L}} |M| \\
&\leq \frac{m^{d-1}}{|G_0|^d} \sum_{S\in\mathcal{S}} |\mathrm{Aut}(S)| \\
&\leq \frac{m^{d-1}s}{|G_0|^d} \sum_{S\in\mathcal{S}} |S| \\
&\leq \frac{m^{d-1}s}{|G_0|^d} \sum_{S\in\mathcal{S}(G_0)} |S|
\end{aligned}$$

and so by Lemma 3.2.11,

$$\begin{aligned}
\sum_{M\in\mathcal{L}} \frac{1}{[G:M]^d} &\leq \frac{m^{d-1}s}{|G_0|^d}|G_0|i(G_0) \\
&\leq \frac{i(G_0)m^{d-1}s}{|G_0|^{d-1}}.
\end{aligned}$$

For all $S \in \mathcal{S}$, $|S| \leq m$ and so by Lemma 2.3.2, $s \leq (6/7)\log m$ giving the second bound.

Similarly,

$$\begin{aligned}\sum_{M\in\mathcal{L}} \frac{1}{[G:M]^d} &\leq \sum_{M\in\mathcal{L}} \frac{|M|^d}{|G_0|^d} \\ &\leq \frac{m^{d-1}}{|G_0|^d} \sum_{S\in\mathcal{S}} |\mathrm{Aut}(S)| \\ &\leq \frac{c}{|G_0|^d} \sum_{S\in\mathcal{S}(G_0)} |S| \\ &\leq \frac{i(G_0)c}{|G_0|^{d-1}}\end{aligned}$$

giving the final inequality. □

We may bound $P_{G,N}(d+1)$ below by $P_{G,N}(d)$. This will simplify the proof when we seek a lower bound for $P_{G,G_0}(3)$, as we will already have bounds for $P_{G,G_0}(2)$.

Lemma 3.2.13. *Let G be a group such that $d(G/N) \leq d$, and suppose N is a normal subgroup of G. Then*

$$P_{G,N}(d+1) \geq P_{G,N}(d).$$

Proof. Suppose $\langle g_1, g_2, \ldots, g_d, N\rangle = G$ for some $g_1, g_2, \ldots, g_d \in G$ and let

$$\Omega_d = \{(n_1, n_2, \ldots, n_d) \in N^d : \langle g_1 n_1, \ldots, g_d n_d\rangle = G\}.$$

By Proposition 3.2.4,

$$P_{G,G_0}(d) = \frac{|\Omega_d|}{|N|^d}.$$

Next define

$$\Omega_{d+1} = \{(n_1, \ldots, n_d, n_{d+1}) \in N^{d+1} : \langle g_1 n_1, \ldots, g_d n_d, n_{d+1}\rangle = G\}.$$

Then as $\langle g_1, g_2, \ldots, g_d, 1, N\rangle = G$, again by Proposition 3.2.4,

$$P_{G,G_0}(d+1) = \frac{|\Omega_{d+1}|}{|N|^{d+1}}.$$

Note that

$$\Omega_d \times N = \{(n_1, \ldots, n_d, n_{d+1}) \in N^{d+1} : \langle g_1 n_1, \ldots, g_d n_d\rangle = G\} \subseteq \Omega_{d+1}.$$

Then

$$P_{G,G_0}(d+1) = \frac{|\Omega_{d+1}|}{|N|^{d+1}} \geq \frac{|\Omega_d \times N|}{|N|^{d+1}} = \frac{|\Omega_d|}{|N|^d} = P_{G,G_0}(d).$$

□

3.3 Calculating $P_{G,G_0}(d)$ for small groups

For some small almost simple groups G with socle G_0, the generic bounds we obtain for $P_{G,G_0}(2)$ will not quite be good enough to show $P_{G,G_0}(2) \geq 53/90$. We also wish to determine exact probabilities for those groups with $P_{G,G_0}(2) \leq 0.9$. We calculate exact values or lower bounds computationally.

Let N be a normal subgroup of G. From Equation 3.1.1

$$P_{G,G_0}(d) = \frac{\phi_G(d)}{|G_0|^d \phi_{G/G_0}(d)}.$$

For any group G, the function `EulerianFunction` in GAP [28] gives $\phi_G(d)$, the number of d-tuples generating G. This method is fast if the table of marks is available in GAP for the group G, and tables of marks are available for many small almost simple groups [74]. Otherwise $\phi_G(d)$ can be estimated by iterating through all d-tuples $(x_1, x_2, \ldots, x_d) \in G^d$, and determining which ones generate G. This method can be improved by noting that $(x_1, x_2, \ldots, x_d)$ generates G if and only if $(x_1^g, x_2^g, \ldots, x_d^g)$ generates G for all $g \in G$. Then, we may iterate through all d-tuples $(x_1, x_2, \ldots, x_d)$ where x_1 is a conjugacy class representative for each conjugacy class of G, and $x_2, \ldots, x_d \in G$. Then if $(x_1, x_2, \ldots, x_d)$ generates G, there are $[G : C_G(x_1)]$ d-tuples of the form $(x_1^g, x_2^g, \ldots, x_d^g)$ in G^d generating G, where $[G : C_G(x_1)]$ is the size of the conjugacy class containing x_1.

For larger groups, particularly those whose table of marks is not available, we may estimate the probability by obtaining maximal subgroups in GAP [28] or Magma [8] and using Lemma 3.2.6. Let H be one of the quasisimple classical groups $\mathrm{SL}_n(q)$, $\mathrm{Sp}_n(q)$, $\mathrm{SU}_n(q)$, $\Omega_n(q)$, $\Omega_n^{\pm}(q)$ in dimension $n \leq 12$. The function `ClassicalMaximals` in Magma [8] allows us to obtain a set $\mathcal{L}$ of conjugacy class representatives for subgroups L of H where L is maximal or $L = M \cap H$, for M a novelty maximal subgroup of a subgroup of $\mathrm{Aut}(H)$. If $G_0 = H/Z(H)$, and $G_0 \leq G \leq \mathrm{Aut}(G_0)$ is d-generated, by Lemma 3.2.9

$$P_{G,G_0}(d) \geq 1 - \sum_{L \in \mathcal{L}} \frac{1}{[H : L]^{d-1}}.$$

Then if G_0 is a simple classical group in dimension at most 12, we may estimate $P_{G,G_0}(2)$ for any G such that $\mathrm{Soc}(G) = G_0$ using Magma [8].

For some other small almost simple groups, there is maximal subgroup information available (usually in the Atlas or Online Atlas [94]), and this can be used to estimate the probability.

In all cases we will round down decimal values of probabilities (actual values or lower bounds) to three decimal places, as we are interested in bounding probabilities below.

3.4 Existing results

Netto conjectured in [75] that the probability that pairs of elements from S_n generate A_n or S_n tends to 1 as $n \to \infty$. Dixon [22] proved this result from which it follows that $P_{G_0}(2) \to 1$ as $|G_0| \to \infty$ for $G_0 = A_n$. Dixon conjectured that this was true for all simple groups. This was proved for classical groups and some exceptional groups in [40]. It was proved for the remaining exceptional groups, and hence for all simple groups in [62]. This result only considers the limit as $|G_0|$ tends to infinity, so the sporadic groups are not considered here. In fact the result proved is slightly stronger. For an almost simple group G with socle G_0, let $P(G)$ denote the probability that two randomly chosen elements of G generate a subgroup containing G_0. Note that $P(G_0) = P_{G_0}(2)$. Together [22], [40], and [62] prove the following.

Theorem 3.4.1 ([62]). *Let G be a finite almost simple group. Then $P(G) \to 1$ as $|G| \to \infty$.*

The proofs in [40] and [62] use the bound

$$P(G) \geq 1 - \sum_{L \in \mathcal{L}} \frac{1}{[G : L]},$$

where $\mathcal{L}$ is a set of conjugacy class representatives for subgroups L of G which are maximal subject to not containing G_0. Then $\mathcal{M} \subseteq \mathcal{L}$, where $\mathcal{M}$ is a set of conjugacy class representatives for maximal subgroups of G not containing G_0. As we bound

$$P_{G,G_0}(2) \geq 1 - \sum_{M \in \mathcal{M}} \frac{1}{[G : M]},$$

we might hope to use these results from [40] and [62] to bound the probability. As we shall describe in Chapters 5 and 6, these results are not quite good enough to bound $P_{G,G_0}(2)$, but we shall use many of the same ideas as [40] and [62] to estimate $P_{G,G_0}(2)$ for classical and exceptional groups.

Now consider the case where $G_0 = A_n$, and suppose $G = A_n$ or S_n. Then [22] proves $P(G) \to 1$ as $n \to \infty$. The proof considers pairs $(x, y) \in G^2$ and considers 3 cases for $\langle x, y \rangle$: where it is intransitive; where it is imprimitive, and where it is primitive. The first 2 cases have a combinatorial proof, and the primitive case uses a theorem of Jordan which states that a primitive subgroup is equal to A_n or S_n if it contains a p-cycle for some prime $p \leq n-3$. The proportion of p-cycles is estimated using theorems of Erdös–Turán [25]. Explicit bounds are obtained for $P(G)$ in terms of n, but they only hold for 'large n' (much larger than $n = 4095$, which is the limit of what we can compute with). These results were improved in [7] and further in [4]. In both these cases the estimates for intransitive and imprimitive groups are used from [22], but improved estimates are used in the primitive case. However,

the bounds for $P(G)$ are given with 'big-O' terms, and so we cannot use these results to find an explicit lower bound for $P(G)$. More precise bounds are obtained in [23] and [70], in particular, [70] gives upper and lower bounds for $P(G)$ which are valid for $n \geq 4$.

Theorem 3.4.2 ([70]). *Let $G = A_n$ or S_n for $n \geq 4$, and let $P(G)$ denote the probability that a random pair of elements generates A_n or S_n. Then*

$$1 - \frac{1}{n} - \frac{13}{n^2} \leq P(G) \leq 1 - \frac{1}{n} + \frac{2}{3n^2}.$$

Looking at this proof in more detail, it in fact shows that $P_{S_n,A_n}(2) \geq 1 - 1/n - 13/n^2$. This result appeared after our calculations were completed, and our calculations give an asymptotically better lower bound so we have included them. In fact our calculations give a better lower bound for $n \geq 65$.

Chapter 4

The probability of generating an almost simple group with socle A_n

In this chapter we prove the following.

Theorem 4.0.1. *Let G be an almost simple group with socle A_n. Then $P_{G,A_n}(2) \geq 53/90 = 0.58\dot{8}$, with equality if and only if $G = A_6$ or S_6. Additionally $P_{G,A_n}(2) > 9/10$ except in the following cases.*

1. *$53/90 \leq P_{G,A_n}(2) \leq 8/10$ if and only if G is one of the following 6 groups: A_5, S_5, A_6, S_6, A_7, A_8.*

2. *$8/10 < P_{G,A_n}(2) \leq 9/10$ if and only if G is one of the following 11 groups: $\mathrm{PGL}_2(9)$, M_{10}, $A_6.2^2$, S_7, S_8, A_9, S_9, A_{10}, S_{10}, A_{11}, S_{11}.*

Theorem 4.9.1 gives a lower bound on $P_{G,A_n}(2)$ in terms of n, and we calculate precise probabilities using GAP [28] for $5 \leq n \leq 13$. These are given in Table 4.1, where all decimal values are rounded down to three decimal places.

If G is an almost simple group with socle A_6, then G is one of $A_6 \cong \mathrm{PSL}_2(9)$, S_6, $\mathrm{PGL}_2(9)$, M_{10}, or $\mathrm{Aut}(A_6) = A_6.2^2$ and the exact value of $P_{G,A_6}(2)$ has been calculated. Otherwise if G is an almost simple group with socle A_n for $n \neq 6$, then $\mathrm{Aut}(A_n) = S_n$, and G is either A_n or S_n. So for the rest of this section we may assume that G is either A_n or S_n.

We bound $P_{G,A_n}(2)$ below using a modification of the ideas of Lemmas 3.2.2 and 3.2.6. For smaller values of n (less than 64), we calculate exact values or lower bounds for $P_{G,A_n}(2)$ computationally.

Lemma 4.0.2. *Let $G = S_n$ or A_n. Let $Q_1(G)$ denote the probability that a random pair of permutations in G generates an intransitive subgroup, given*

G	$P_{G,A_n}(2)$	$P_{G,A_n}(2)$
A_5	19/30	0.633
S_5	19/30	0.633
A_6	53/90	0.588
S_6	53/90	0.588
M_{10}	13/15	0.866
$\mathrm{PGL}_2(9)$	13/15	0.866
$A_6.2^2$	13/15	0.866
A_7	229/315	0.726
S_7	103/126	0.817
A_8	133/180	0.738
S_8	4111/5040	0.815
A_9	15403/18144	0.848
S_9	78293/90720	0.863
A_{10}	29401/33600	0.875
S_{10}	29401/33600	0.875
A_{11}	743249/831600	0.893
S_{11}	4462987/4989600	0.894
A_{12}	108057583/119750400	0.902
S_{12}	9830941/10886400	0.903
A_{13}	129271277/141523200	0.913
S_{13}	284397779/311351040	0.913

Table 4.1: Exact values for $P_{G,A_n}(2)$ where $\mathrm{Soc}(G) = A_n$ and $5 \leq n \leq 13$

that the pair generates G modulo A_n. Then

$$P_{G,A_n}(2) \geq 1 - Q_1(G) - \sum_{\substack{M <_{\max} G \\ M \text{ transitive} \\ M \neq A_n}} \frac{1}{[G:M]^2}.$$

Proof. Let $Q_2(G)$ denote the probability that a random pair of permutations in G generates a proper transitive subgroup of G given that it generates G modulo A_n. If $(g_1, g_2) \in G^2$ generates G modulo A_n, then it either generates G, generates an intransitive subgroup of G, or generates a proper transitive subgroup of G. Then

$$P_{G,A_n}(2) \geq 1 - Q_1(G) - Q_2(G).$$

Now we bound $Q_2(G)$. Note that if $(g_1, g_2) \in G^2$ generates G modulo A_n, $\langle g_1, g_2 \rangle \neq G$, and $\langle g_1, g_2 \rangle$ is transitive, then $\langle g_1, g_2 \rangle \leq M$ for some transitive maximal subgroup M of G where $M \neq A_n$. First suppose $G = A_n$. Then

$$\begin{aligned} Q_2(G) &= \frac{|\{(g_1,g_2) \in G^2 : \langle g_1, g_2 \rangle \neq G \text{ transitive}\}|}{|G|^2} \\ &\leq \frac{|\{(g_1,g_2) \in G^2 : \langle g_1, g_2 \rangle \leq M, M \text{ transitive}, M <_{\max} G\}|}{|G|^2} \\ &\leq \sum_{\substack{M <_{\max} G \\ M \text{ transitive} \\ M \neq A_n}} \frac{|M|^2}{|G|^2}. \end{aligned}$$

Now suppose $G = S_n$. Then $(g_1, g_2) \in G^2$ generates a proper transitive subgroup of G and generates G modulo A_n if $\langle g_1, g_2 \rangle \leq M$ for a transitive maximal subgroup of G and at least one of g_1 and g_2 is odd. Then

$$Q_2(G) = \frac{|\{(g_1,g_2) \in G^2 : \langle g_1, g_2 \rangle \neq G \text{ transitive, } g_1 \text{ or } g_2 \text{ odd}\}|}{|\{(g_1,g_2) \in G^2 : g_1 \text{ or } g_2 \text{ odd }\}|}.$$

Note that

$$|\{(g_1,g_2) \in G^2 : g_1 \text{ or } g_2 \text{ odd}\}| = (3/4)|G|^2.$$

Similarly 3/4 of pairs (m_1, m_2) in M^2, for $M \neq A_n$ a transitive maximal subgroup of G, have at least one of m_1 or m_2 odd. Then

$$\begin{aligned} Q_2(G) &\leq \frac{|\{(g_1,g_2) \in M^2 : M <_{\max} G, M \text{ transitive, } g_1 \text{ or } g_2 \text{ odd}\}|}{(3/4)|G|^2} \\ &\leq \sum_{\substack{M <_{\max} G \\ M \text{ transitive} \\ M \neq A_n}} \frac{(3/4)|M|^2}{(3/4)|G|^2} \\ &= \sum_{\substack{M <_{\max} G \\ M \text{ transitive} \\ M \neq A_n}} \frac{|M|^2}{|G|^2}. \end{aligned}$$

Then the result follows for $G = A_n$ or S_n. □

We estimate $Q_1(G)$ using the ideas of [70, Lemma 2.2]. The remaining sum requires us to estimate the number (in most cases we calculate the number up to conjugacy) and order of transitive maximal subgroups of G.

Now we give a brief overview of the method we use before considering each type of transitive maximal subgroup separately. Consider maximal transitive subgroups of G which do not contain A_n. Then these maximal subgroups are described by the O'Nan–Scott Theorem (Theorem 2.1.24). Let X be one of the following groups:

- $S_m \operatorname{wr} S_k$ with $n = mk$, $m > 1$, $k > 1$;
- $\mathrm{AGL}_k(p)$ with $n = p^k$;
- $T^k.(\mathrm{Out}(T) \times S_k)$ where $k \geq 2$, $n = |T|^{k-1}$, T non-abelian simple;
- $S_m \operatorname{wr} S_k$ where $n = m^k$, $m \geq 5$, $k > 1$.

For each given type of subgroup, and a given k (and T in the diagonal case), there is one conjugacy class of such subgroups in S_n as stated in [85]. So, if $M \neq A_n$ is a maximal subgroup of G which is not almost simple, then $M = X \cap G$ for some X in the list. We consider each possibility for X and calculate the index of $X \cap G$ in G ($X \cap G$ may or may not be maximal in G).

The following is a more precise version of Lemma 3.2.8 where we determine how conjugacy classes in S_n split over A_n.

Lemma 4.0.3. *Let H be a subgroup of $A_n < S_n$. Then*

$$[S_n : N_{S_n}(H)] \leq 2[A_n : N_{A_n}(H)].$$

If $N_{S_n}(H)$ contains an odd permutation then $[S_n : N_{S_n}(H)] = [A_n : N_{A_n}(H)]$.

Proof. The index of the normaliser of H in A_n is given by

$$\begin{aligned} [A_n : N_{A_n}(H)] &= [A_n : A_n \cap N_{S_n}(H)] \\ &= [A_n N_{S_n}(H) : N_{S_n}(H)]. \end{aligned}$$

If $N_{S_n}(H)$ contains an odd permutation, the maximality of A_n in S_n implies $A_n N_{S_n}(H) = S_n$. Then

$$[A_n : N_{A_n}(H)] = [S_n : N_{S_n}(H)].$$

Otherwise,

$$[A_n : N_{A_n}(H)] = \frac{1}{2}[S_n : N_{S_n}(H)].$$

□

This lemma tells us that if we have a subgroup of A_n (and therefore of S_n) then the conjugacy classes of this subgroup in S_n may split over A_n. If X (as defined above) contains an odd permutation, then by the maximality of A_n in S_n, $A_nX = S_n$, and so $[S_n : X] = [A_n : X \cap A_n]$. In this case $X \leq N_{S_n}(X \cap A_n)$ and so by Lemma 4.0.3 the number of conjugates of X in S_n is equal to the number of conjugates of $X \cap A_n$ in A_n.

Otherwise X does not contain an odd permutation and so $X = X \cap A_n = X \cap S_n$. Then X cannot be maximal in S_n, but may be maximal in A_n. In this case conjugacy classes of X in S_n may split over A_n.

Next we consider almost simple maximal subgroups of A_n or S_n.

Theorem 4.0.4 ([52])**.** *Let M be primitive of degree n on Ω with $\mathrm{Soc}(M) = T$, a non-abelian simple group. Then one of the following holds:*

1. *$T = A_m$ acting on k-subsets of $\{1, \ldots, m\}$ or on partitions of $\{1, \ldots, m\}$ into l subsets of size k, where $lk = m$, $l > 1$, $k > 1$; $n = \binom{m}{k}$ or $m!/(k!)^l l!$ respectively;*

2. *T is a classical simple group acting on an orbit of subspaces of the natural module, or (in the case $T = \mathrm{PSL}_d(q)$) pairs of subspaces of complementary dimensions;*

3. *$|M| \leq n^c$, where we may take $c = 6.077948094$.*

The original statement of this theorem in [52] gives the value of $c = 9$. An unpublished result of Liebeck stated in [11, Theorem 4.14] improves this result to $c = 6.077948094$.

So if M is an almost simple maximal subgroup of G, then either $T = \mathrm{Soc}(M)$ is alternating or classical with a described action, or $|M|$ is 'small'. In the first two cases the action of T on n points is described and we determine the number of such subgroups up to conjugacy, and the order of these subgroups in terms of n in a similar way to before. In the final case we consider possibilities for T, and use the fact that $T \leq S_n$ if and only if T has a permutation representation of degree n.

We now consider each type of maximal subgroup from Theorem 2.1.24 and Theorem 4.0.4 in turn.

4.1 Intransitive maximal subgroups

For $G = A_n$ or S_n we estimate $Q_1(G)$, the probability that a random pair in G^2 generates an intransitive subgroup of G, given that the pair generates G modulo A_n. We estimate this using the ideas of [70, Lemma 2.2].

Lemma 4.1.1. *Let $G = A_n$ or S_n and let $Q_1(G)$ denote the probability that a random pair of permutations in G generates an intransitive subgroup of*

G, given that it generates G modulo A_n. Then

$$Q_1(G) \leq \frac{1}{n} + \frac{3}{2n(n-1)} + \frac{3}{(n-1)(n-2)}.$$

Proof. Let $\Omega = \{1, \ldots, n\}$. If $(x, y) \in G^2$ generates an intransitive subgroup of G, then

$$\langle x, y \rangle \leq S_A \times S_{\Omega \setminus A}$$

for some $A \subseteq \Omega$ where $1 \leq |A| \leq \lfloor n/2 \rfloor$. Note that $\langle x, y \rangle \leq S_A \times S_{\Omega \setminus A}$ if and only if $x \in S_A \times S_{\Omega \setminus A}$ and $y \in S_A \times S_{\Omega \setminus A}$. Also $S_A \times S_{\Omega \setminus A} \cong S_k \times S_{n-k}$ for some k. For a given k, the number of subgroups of the form $S_A \times S_{\Omega \setminus A} \leq G$ is the number of k subsets $A \subseteq \Omega$, which is $\binom{n}{k}$. The even permutations in $S_A \times S_{\Omega \setminus A}$ are precisely those elements contained in $(S_A \times S_{\Omega \setminus A}) \cap A_\Omega$. This subgroup has index 2 in $S_A \times S_{\Omega \setminus A}$. Thus, precisely a quarter of all pairs $(x, y) \in (S_A \times S_{\Omega \setminus A})^2$ have both x and y even and therefore three-quarters of all pairs have at least one of x or y odd.

First suppose $G = S_n$. Define the following subsets of G^2 for $1 \leq k \leq \lfloor n/2 \rfloor$,

$$P_k = \{(x, y) \in G^2 : \langle x, y \rangle \leq S_A \times S_{\Omega \setminus A}, A \subseteq \Omega, |A| = k, x \text{ or } y \text{ odd}\}.$$

As $(x, y) \in G$ generates G modulo A_n if and only if at least one of x, y is odd, then

$$Q_1(G) = \frac{|\{(x, y) \in G^2 : \langle x, y \rangle \text{ intransitive}, x \text{ or } y \text{ odd}\}|}{|\{(x, y) \in G^2 : x \text{ or } y \text{ odd}\}|}.$$

Note that

$$|\{(x, y) \in G^2 : x \text{ or } y \text{ odd}\}| = (3/4)|G|^2.$$

Then

$$Q_1(G) = \frac{|\bigcup_{k=1}^{\lfloor n/2 \rfloor} P_k|}{(3/4)|G|^2}.$$

We bound the numerator as follows,

$$|\bigcup_{k=1}^{\lfloor n/2 \rfloor} P_k| \leq |P_1| + |P_2 \setminus P_1| + \sum_{k=3}^{\lfloor n/2 \rfloor} |P_k|.$$

The size of P_k is

$$\begin{aligned} |P_k| &\leq \binom{n}{k} \times (3/4)|S_A \times S_{\Omega \setminus A}|^2 \\ &= \binom{n}{k} (3/4)((n-k)!k!)^2 \\ &= \frac{3n!(n-k)!k!}{4}. \end{aligned}$$

Now we bound $|P_2 \setminus P_1|$. Suppose $A \subseteq \Omega$ such that $|A| = 2$. If $x, y \in S_A \times S_{\Omega\setminus A} \leq S_n$ then $x = (\sigma_1, \rho_1)$ and $y = (\sigma_2, \rho_2)$ for $\sigma_1, \sigma_2 \in S_A$ and $\rho_1, \rho_2 \in S_{\Omega\setminus A}$. For $(x, y) \in P_2$, at least one of x or y must be odd. Then $(x, y) \in P_1$ if $\sigma_1 = \sigma_2 = 1$. Thus at least a quarter of the elements in P_2 are contained in P_1 and so $|P_2 \setminus P_1| \leq \frac{3}{4}|P_2|$.

So the proportion of pairs in G^2 that generate an intransitive subgroup of G, given they generate G modulo A_n is

$$\begin{aligned}
Q_1(G) &\leq \frac{|\bigcup_{k=1}^{\lfloor n/2\rfloor} P_k|}{(3/4)|G|^2} \\
&\leq \frac{4}{3(n!)^2}\big(|P_1| + |P_2 \setminus P_1| + \sum_{k=3}^{\lfloor n/2\rfloor} |P_k|\big) \\
&\leq \frac{4}{3(n!)^2}\big(|P_1| + \frac{3}{4}|P_2| + \sum_{k=3}^{\lfloor n/2\rfloor} |P_k|\big) \\
&\leq \frac{1}{(n!)}\big((n-1)! + \frac{3}{4}(n-2)!2! + \sum_{k=3}^{\lfloor n/2\rfloor} (n-k)!k!\big) \\
&= \frac{1}{n} + \frac{3}{2n(n-1)} + \sum_{k=3}^{\lfloor n/2\rfloor} \binom{n}{k}^{-1} \\
&= \frac{1}{n} + \frac{3}{2n(n-1)} + (\lfloor n/2\rfloor - 2)\frac{(n-3)!3!}{n!} \\
&\leq \frac{1}{n} + \frac{3}{2n(n-1)} + \frac{3}{(n-1)(n-2)}.
\end{aligned}$$

This concludes the proof in the case where $G = S_n$.

Now suppose $G = A_n$. Then $Q_1(G)$ is the probability a random pair of elements in G^2 generates an intransitive subgroup of G, and the result is immediate from [70, Lemma 2.2]. □

4.2 Imprimitive maximal subgroups

Let M be an imprimitive maximal subgroup of $G = A_n$ or S_n. By Theorem 2.1.24

$$M = (S_m \mathrm{wr} S_k) \cap G,$$

where $mk = n$ and $1 < k < n$.

Lemma 4.2.1. *Let $\mathcal{M}$ be a set of conjugacy class representatives for imprimitive maximal subgroups of $G = A_n$ or S_n. Then*

$$\sum_{M\in\mathcal{M}} \frac{1}{[G : M]} \leq \frac{\sqrt{n}}{2^{n/4-1}}.$$

Proof. Consider an imprimitive subgroup of G of the form $M = (S_m \mathrm{wr} S_k) \cap G$ where $n = mk$ and $1 < k < n$. Up to conjugacy in S_n, there is one subgroup of this form for every k such that $1 < k < n$ and k divides n. As $S_m \,\mathrm{wr}\, S_k$ contains an odd permutation, there is at most one conjugacy class of maximal subgroups of this form in G for each k, and

$$[G : M] = [S_n : S_m \,\mathrm{wr}\, S_k].$$

Then

$$\begin{aligned}
\sum_{M \in \mathcal{M}} \frac{1}{[G : M]} &\leq \sum_{\substack{1<k<n \\ k|n}} \frac{1}{[G : (S_{n/k} \mathrm{wr} S_k) \cap G]} \\
&= \sum_{\substack{1<k<n \\ k|n}} \frac{1}{[S_n : S_{n/k} \mathrm{wr} S_k]} \\
&= \sum_{\substack{1<k<n \\ k|n}} \frac{((n/k)!)^k k!}{n!}.
\end{aligned}$$

As in the proof of [22, Lemma 2] we can approximate the last expression as follows:

$$\begin{aligned}
\frac{(m!)^k k!}{n!} &= \prod_{i=1}^{k} \frac{m! i}{im(im-1)\cdots(im-(m-1))} \\
&= \prod_{i=1}^{k} \prod_{j=1}^{m-1} \frac{m-j}{im-j} \\
&\leq \prod_{i=1}^{k} \prod_{j=1}^{m-1} \frac{1}{i} \\
&= \frac{1}{(k!)^{m-1}} \\
&\leq \frac{1}{(2^{k/2})^{m-1}} \text{ since } k > 1 \\
&\leq \frac{1}{(2^{k/2})^{m/2}} \text{ since } m > 1 \\
&= \frac{1}{2^{n/4}}.
\end{aligned}$$

The number of possible k's, that is, the number of proper divisors of n is less than $2\sqrt{n}$ and so,

$$\sum_{M \in \mathcal{M}} \frac{1}{[G : M]} \leq \sum_{\substack{1<k<n \\ k|n}} \frac{1}{2^{n/4}} \leq \frac{\sqrt{n}}{2^{n/4-1}}.$$

□

4.3 Maximal subgroups of affine type

Let M be a maximal subgroup of $G = A_n$ or S_n of affine type so that

$$M = \mathrm{AGL}_k(p) \cap G,$$

and $n = p^k$. By Lemma 2.2.4

$$|\mathrm{AGL}_k(p)| = p^k \prod_{i=0}^{k-1} (p^k - p^i).$$

Lemma 4.3.1. *Let $\mathcal{M}$ be a set of conjugacy class representatives for maximal subgroups of affine type in $G = A_n$ or S_n. Then*

$$\sum_{M \in \mathcal{M}} \frac{1}{[G : M]} \leq \frac{4}{(n - \lfloor \log n \rfloor - 1)!}.$$

Proof. Maximal subgroups of affine type are of the form $M = \mathrm{AGL}_k(p) \cap G$ for $n = p^k$ for some prime p. There is at most one conjugacy class in S_n of subgroups of the form $\mathrm{AGL}_k(p) \cap G$ as $n = p^k$ for at most one possibility for p.

It may be that $\mathrm{AGL}_k(p)$ does not contain an odd permutation. In this case $\mathrm{AGL}_k(p) \leq A_n$, and by Lemma 4.0.3 there are 2 conjugacy classes of such maximal subgroups in A_n. In this case $\mathrm{AGL}_k(p)$ is not maximal in S_n, but may be maximal in A_n. If $\mathrm{AGL}_k(p)$ does contain an odd permutation, $\mathrm{AGL}_k(p) \cap G$ may be maximal when G is either A_n or S_n, and there is one conjugacy class of such subgroups in G.

Then

$$[G : \mathrm{AGL}_k(p) \cap G] \geq \frac{1}{2}[S_n : \mathrm{AGL}_k(p)],$$

and

$$\begin{aligned} [S_n : \mathrm{AGL}_k(p)] &= \frac{n!}{p^k \prod_{i=0}^{k-1}(p^k - p^i)} \\ &= \frac{n!}{n(n-1)\prod_{i=1}^{k-1}(p^k - p^i)} \\ &= \frac{(n-2)!}{\prod_{i=1}^{k-1}(n - p^i)}. \end{aligned}$$

Now, as $p^i \geq i + 1$ for all $i \in \mathbb{N}$, we obtain $(n - (i+1)) \geq (n - p^i)$. Then

$$[S_n : \mathrm{AGL}_k(p)] \geq (n - k - 1)!.$$

We bound $k \leq \lfloor \log n \rfloor$ as $n = p^k \geq 2^k$ and k is an integer. Then

$$[S_n : \mathrm{AGL}_k(p)] \geq (n - \lfloor \log n \rfloor - 1)!$$

and so

$$[G : \mathrm{AGL}_k(p) \cap G] \geq \frac{1}{2}(n - \lfloor \log n \rfloor - 1)!$$

Then

$$\sum_{M \in \mathcal{M}} \frac{1}{[G : M]} \leq \frac{4}{(n - \lfloor \log n \rfloor - 1)!}.$$

□

4.4 Maximal subgroups of diagonal type

Let M be a maximal subgroup of $G = A_n$ or S_n of diagonal type. Then

$$M = (T^k.(S_k \times \mathrm{Out}(T))) \cap G$$

where T is a non-abelian simple group. Here, the degree is $n = |T|^{k-1}$.

Lemma 4.4.1. *Let $\mathcal{M}$ be a set of conjugacy class representatives for maximal subgroups of $G = A_n$ or S_n of diagonal type. Then*

$$\sum_{M \in \mathcal{M}} \frac{1}{[G : M]} \leq \frac{8n(\log n)(\lfloor \log_{60} n \rfloor + 1)!}{(n-1)!}.$$

Proof. Consider a subgroup of G of the form $(T^k.(S_k \times \mathrm{Out}(T))) \cap G$. For a given simple group T, maximal subgroups of this form with the diagonal action are conjugate in S_n. Up to conjugacy in S_n, the number of subgroups of this form is therefore equal to the number of possible simple groups T up to isomorphism. As $n = |T^k|$, then by Theorem 2.3.4 there are at most two conjugacy classes of such maximal subgroups in S_n. By Lemma 4.0.3 conjugacy classes may split over A_n. Then the number of conjugacy classes of maximal subgroups of G of diagonal type is at most 4.

Next we estimate the index. As $n = |T|^{k-1}$ and $k \geq 2$, we have $|T|^k \leq n^2$ and using Lemma 2.3.2

$$|\mathrm{Out}(T)| \leq \log |T| \leq \log n.$$

Now

$$k - 1 = \log_{|T|} n \leq \log_{60} n$$

and so

$$k \leq \log_{60} n + 1.$$

As k is an integer $k \leq \lfloor \log_{60} n \rfloor + 1$. Then

$$|S_k| \leq (\lfloor \log_{60} n \rfloor + 1)!$$

and then an estimate for the order of this subgroup is

$$|T^k.(S_k \times \mathrm{Out}(T))| \leq n^2(\log n)(\lfloor \log_{60} n \rfloor + 1)!.$$

Then the index is

$$\begin{aligned}[G : (T^k.(S_k \times \mathrm{Out}(T))) \cap G] &\geq \frac{1}{2}[S_n : (T^k.(S_k \times \mathrm{Out}(T)))] \\ &= \frac{n!}{2n^2(\log n)(\lfloor \log_{60} n \rfloor + 1)!} \\ &= \frac{(n-1)!}{2n(\log n)(\lfloor \log_{60} n \rfloor + 1)!}\end{aligned}$$

so,

$$\begin{aligned}\sum_{M \in \mathcal{M}} \frac{1}{[G : M]} &\leq 4 \times \frac{2n(\log n)(\lfloor \log_{60} n \rfloor + 1)!}{(n-1)!} \\ &= \frac{8n(\log n)(\lfloor \log_{60} n \rfloor + 1)!}{(n-1)!}.\end{aligned}$$

□

4.5 Maximal subgroups of product type

Let M be a maximal subgroup of $G = A_n$ or S_n of product action type. Then

$$M = (S_m \mathrm{wr} S_k) \cap G$$

where $n = m^k$.

Lemma 4.5.1. *Let $\mathcal{M}$ be a set of conjugacy class representatives for maximal subgroups of $G = A_n$ or S_n which are of product action type. Then*

$$\sum_{M \in \mathcal{M}} \frac{1}{[G : M]} \leq \frac{1}{n^{n/3}}.$$

Proof. Maximal subgroups of G of product action type are of the form $(S_m \,\mathrm{wr}\, S_k) \cap G$ for $n = m^k$, where $m \geq 5$, $k \geq 2$ and $n \geq 25$. Then $k = \log_m n \leq \log_5 n$ and $m = n^{1/k} \leq \sqrt{n}$.

First we determine an upper bound on the number of conjugacy classes of maximal subgroups of product type. The number of subgroups of the form $(S_m \,\mathrm{wr}\, S_k) \cap G$ up to conjugacy in S_n is the same as counting the number of ways we can write $n = m^k$ for some m and k. Write n as a product of primes, $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_t^{\alpha_t}$ for distinct primes p_i, and $\alpha_i \in \mathbb{N}$. If $n = m^k$ for some m and k, then $m = p_1^{\alpha_1/k} \dots p_t^{\alpha_t/k}$ for some k that divides α_i for $1 \leq i \leq t$. Now choose s to be the greatest common divisor of $\alpha_1, \dots, \alpha_t$, and let $d = p_1^{\alpha_1/s} \dots p_t^{\alpha_t/s}$. Then k must divide s. So the number of ways of writing $n = m^k$ for some m and k is the number of divisors of s. This is bounded by s itself. We use the fact that $n = d^s \geq 2^s$ to bound $s \leq \log n$.

By Lemma 4.0.3 the conjugacy classes of $(S_m \operatorname{wr} S_k) \cap A_n$ may split over A_n. Then, the number of conjugacy classes of maximal subgroups of product action type in G is at most $2 \log n$.

The order of $|S_m \operatorname{wr} S_k|$ may be bounded as follows,

$$\begin{aligned} |S_m \operatorname{wr} S_k| &= (m!)^k k! \\ &\leq (m^m)^k k^k \\ &= n^m k^k \\ &\leq n^{\sqrt{n}} (\log_5 n)^{\log_5 n}. \end{aligned}$$

Using an version of Stirling's Formula which gives explicit bounds (Lemma 2.4.4,

$$n! \geq e^{7/8} \left(\frac{n}{e}\right)^n \sqrt{n}.$$

Note that as $S_m \operatorname{wr} S_k$ may not contain an odd permutation

$$[G : M] \geq \frac{1}{2} [S_n : S_m \operatorname{wr} S_k].$$

Then,

$$\sum_{M \in \mathcal{M}} \frac{1}{[G : M]} \leq \frac{4(\log n) n^{\sqrt{n}} (\log_5 n)^{\log_5 n}}{e^{7/8} (\frac{n}{e})^n \sqrt{n}}.$$

As $n \geq 25 > e^3$, then we obtain the following estimates, $e^n \leq n^{n/3}$, $\log n \leq \sqrt{n} \leq n/5$, $\log_5 n \leq n^{1/3}$ and $\log_5 n \leq n/10$. Then

$$\begin{aligned} \sum_{M \in \mathcal{M}} \frac{1}{[G : M]} &\leq \frac{4(\log n) n^{\sqrt{n}} (\log_5 n)^{\log_5 n}}{e^{7/8} (\frac{n}{e})^n \sqrt{n}} \\ &\leq \frac{2\sqrt{n} (n^{\sqrt{n}}) (\log_5 n)^{\log_5 n} e^n}{n^n \sqrt{n}} \\ &\leq \frac{2 n^{n/5} (n^{1/3})^{n/10} n^{n/3}}{n^n} \\ &\leq \frac{2 n^{17n/30}}{n^n} \\ &\leq \frac{1}{n^{n/3}}. \end{aligned}$$

□

4.6 Maximal subgroups of A_n or S_n of the form A_m or S_m acting on subsets or partitions

Let H be an almost simple subgroup of S_n such that $H \cong S_m$ arising from the action of S_m on k-sets. Then H acts on the set of all subsets of $\{1, 2, \ldots, m\}$

of size k. So $n = \binom{m}{k}$ for some $m \geq 5$, $k > 1$. For a given n, a given k determines m (and vice-versa). If $H = S_m$ acting on k-sets, for each k there is at most one such H up to conjugacy in S_n as the action of H on the k-sets is the same (that is, all such groups are permutation isomorphic). It may be that $H \leq A_n$.

Lemma 4.6.1. *Let H be a subgroup of S_n, where $H \cong S_m$ acts on k-subsets of $\{1, \ldots, m\}$. Then $H \leq A_n$ if and only if*

$$\frac{(m-2)!}{(k-1)!(m-k-1)!}$$

is even.

Proof. As H is generated by transpositions, to show that $H \leq A_n$, it suffices to show that a transposition in H (in its action on m points) corresponds to an even permutation (in its action on n points, i.e. in its action on k-sets). Without loss of generality, consider the involution (12) in H (considered in its action on m points). This corresponds to a permutation in S_n, where the permutation consists of one transposition for each pair of k-sets swapped by (12). This is precisely the number of k-sets containing 1 but not 2. The number of k-sets containing 1 is $\binom{m-1}{k-1}$ and the number of k-sets containing both 1 and 2 is $\binom{m-2}{k-2}$. Then, the number of sets containing 1 but not 2 is

$$\begin{aligned}
\binom{m-1}{k-1} - \binom{m-2}{k-2} &= \frac{(m-1)!}{(m-k)!(k-1)!} - \frac{(m-2)!}{(m-k)!(k-2)!} \\
&= \frac{(m-1)! - (m-2)!(k-1)}{(k-1)!(m-k)!} \\
&= \frac{(m-2)!((m-1)-(k-1))}{(k-1)!(m-k)!} \\
&= \frac{(m-2)!}{(k-1)!(m-k-1)!}.
\end{aligned}$$

That is, the transposition $(12) \in H$ corresponds to an even permutation in its action on n points precisely when

$$\frac{(m-2)!}{(k-1)!(m-k-1)!}$$

is even. □

Lemma 4.6.2. *Let $\mathcal{M}$ be a set of conjugacy class representatives for almost simple maximal subgroups of $G = A_n$ or S_n of the form $H \cap G$ where $H \cong S_m$ acting on k-sets of $\{1, \ldots, m\}$. Then*

$$\sum_{M \in \mathcal{M}} \frac{1}{[G:M]} \leq \frac{4(\sqrt{2n}-3)(\lfloor\sqrt{2n}\rfloor+1)!}{n!}.$$

Proof. In this case

$$n = \binom{m}{k} \geq \binom{m}{2} \geq \frac{(m-1)^2}{2}$$

and so

$$m \leq \lfloor \sqrt{2n} \rfloor + 1.$$

For a given m such that $n = \binom{m}{k}$ for some k, there is one conjugacy class of subgroups of this form in S_n, as all subgroups of this form with this action are permutation isomorphic. By Lemma 4.0.3 the number of conjugates of $H \cap A_n$ in A_n is at most twice the number of conjugates of $H \cap A_n$ in S_n, that is, at most twice the number of ways of writing $n = \binom{m}{k}$ for some $m \geq 5$, $k > 1$. Without loss of generality we can take $k \leq \frac{m}{2}$, and for each m there is at most one k. As $5 \leq m \leq \sqrt{2n} + 1$, there are at most $\sqrt{2n} - 3$ different ways of writing n as $\binom{m}{k}$. Then there are at most $2(\sqrt{2n} - 3)$ maximal subgroups of this type up to conjugacy in G.

Then a lower bound for the index is

$$\begin{aligned} [G : G \cap H] &\geq \frac{n!}{2m!} \\ &\geq \frac{n!}{2(\lfloor \sqrt{2n} \rfloor + 1)!}. \end{aligned}$$

Then

$$\begin{aligned} \sum_{M \in \mathcal{M}} \frac{1}{[G : M]} &\leq \frac{2(\sqrt{2n} - 3) \times 2(\lfloor \sqrt{2n} \rfloor + 1)!}{n!} \\ &\leq \frac{4(\sqrt{2n} - 3)(\lfloor \sqrt{2n} \rfloor + 1)!}{n!}. \end{aligned}$$

□

Now we consider $H \cong S_m$ as a subset of S_n, where S_m acts on partitions of $\{1, \ldots, m\}$, into l sets of size k. Then

$$n = \frac{m!}{(k!)^l l!}$$

for some $m \geq 5$ and $l, k > 1$ where $m = lk$. For a given l and m (which determines k), all such subgroups of S_n acting in this way are permutation isomorphic, that is, there is one such conjugacy class of subgroups H in S_n. Again the subgroup H might not contain an odd permutation in its action on n points.

Lemma 4.6.3. *Let H be a subgroup of S_n, where $H \cong S_m$ acting on l subsets of $\{1, 2, \ldots, m\}$ of size k. Then $H \leq A_n$ if and only if*

$$\frac{m(m-k)(m-2)!}{2(k!)^l l!}$$

is even.

Proof. Then H is a subgroup of A_n when a transposition in H (in its action on m points) corresponds to an even permutation in its action on partitions of $\{1,\ldots,m\}$ into l sets of size k (action on n points). Without loss of generality, we consider an involution (12) in H (in its action on m points) and determine when this corresponds to an even permutation in S_n. First consider how many of the l sets of size k contain 1 and 2 in the same k-sets. The number of ways of choosing a k-set containing 1 and 2 is $\binom{m-2}{k-2}$. Then the number of ways of placing the remaining $m-k$ elements into the remaining $l-1$ sets of size k is $\frac{(m-k)!}{(k!)^{l-1}(l-1)!}$. Then the number of l sets of size k containing 1 and 2 in the same set is $\binom{m-2}{k-2} \times \frac{(m-k)!}{(k!)^{l-1}(l-1)!}$. So, the number of points moved by (12) is

$$\begin{aligned} n - \left(\binom{m-2}{k-2} \times \frac{(m-k)!}{(k!)^{l-1}(l-1)!}\right) &= \frac{m!}{(k!)^l l!} - \frac{kl(k-1)(m-2)!}{(k!)^l l!} \\ &= \frac{m(m-k)(m-2)!}{(k!)^l l!}. \end{aligned}$$

This gives the number of points moved by (12). So the corresponding permutation in S_n consists of $\frac{m(m-k)(m-2)!}{2(k!)^l l!}$ disjoint transpositions. Then $H \leq A_n$ precisely when $\frac{m(m-k)(m-2)!}{2(k!)^l l!}$ is even. □

Lemma 4.6.4. *Let $\mathcal{M}$ be a set of conjugacy class representatives for almost simple maximal subgroups of $G = A_n$ or S_n which are of the form $H \cap G$ where $H \cong S_m$ acting on l subsets of $\{1,2,\ldots,m\}$ of size k. Then*

$$\sum_{M \in \mathcal{M}} \frac{1}{[G:M]} \leq \frac{32(\log n)^2(\lfloor 4\log n \rfloor)!}{n!}.$$

Proof. For each group of this form $n = \frac{m!}{(k!)^l l!}$ for some m, k, l. As in the proof of Lemma 4.2.1,

$$\frac{1}{n} = \frac{(k!)^l l!}{m!} \leq \frac{1}{2^{m/4}}.$$

As $2^{m/4} \leq n$, that is, $m \leq 4\log n$, and as m is an integer,

$$m \leq \lfloor 4\log n \rfloor.$$

Then the index is

$$[G : H \cap G] \geq \frac{n!}{2(\lfloor 4\log n \rfloor)!}.$$

Up to conjugacy in S_n, the number of subgroups of the form $H \cap G$ is the number of ways of writing $n = \frac{m!}{(k!)^l l!}$ for some m, k, l. The number of ways of writing $n = \frac{m!}{(k!)^l l!}$ is less than the number of possibilities for k, l and m. As k is determined by l and m, $l \leq m/2$, and $m \leq 4\log n$, the number

of ways of writing n in this form is at most $\frac{1}{2}(4\log n)^2$. So, as conjugacy classes may split over A_n, the number of maximal subgroups of this type up to conjugacy in G is at most $(4\log n)^2$.

Then,

$$\begin{aligned}\sum_{M\in\mathcal{M}} \frac{1}{[G:M]} &\leq (4\log n)^2 \times \frac{2(\lfloor 4\log n\rfloor)!}{n!} \\ &\leq \frac{32(\log n)^2(\lfloor 4\log n\rfloor)!}{n!}.\end{aligned}$$

□

4.7 Maximal subgroups which are almost simple classical groups

Next we consider almost simple maximal subgroups M of $G = A_n$ or S_n where $\mathrm{Soc}(M) = T$ for some simple classical group T, and suppose M acts on subspaces, or pairs of subspaces (as in Theorem 4.0.4). Let T be defined over $\mathbb{F}_q$, and have dimension d, and let V be the natural module. Then if $T = \mathrm{PSU}_d(q)$, $V = \mathbb{F}_{q^2}^d$, otherwise $V = \mathbb{F}_q^d$. Let M act on subspaces $U < V$, or pairs $U, W < V$ of subspaces of complementary dimension where $\dim U = k < d$ and $\dim W = d - k$. As the action of M on the orbit of subspaces is primitive, then M_α, the stabiliser of a subspace, is a maximal subgroup of M. Then the subgroups M_α lie in Aschbacher class $\mathcal{C}_1$, and these subgroups are described in [44, Tables 3.5.A - 3.5.G]. This gives us the following possibilities for M.

1. $T = \mathrm{PSL}_d(q)$
   - M acts on k-dimensional subspaces of V.
   - M acts on pairs of subspaces $U, W < V$, where $U \oplus W = V$.
   - M acts on pairs of subspaces $U, W < V$, where $U < W < V$.
2. $T = \mathrm{PSp}_d(q)$
   - M acts on non-degenerate k-dimensional subspaces.
   - M acts on totally singular k-dimensional subspaces.
3. $T = \mathrm{PSU}_d(q)$
   - M acts on non-degenerate k-dimensional subspaces.
   - M acts on totally singular k-dimensional subspaces .
4. $T = \Omega_d^\circ(q)$

- M acts on k-dimensional singular subspaces.
- M acts on k-dimensional non-degenerate subspaces where k is odd.
- M acts on k-dimensional non-degenerate subspaces U of V for k even, and where U is of plus type.
- M acts on k-dimensional non-degenerate subspaces U of V for k even, and where U is of minus type.

5. $T = \mathrm{P}\Omega_d^+(q)$
   - M acts on k-dimensional singular subspaces.
   - M acts on k-dimensional non-degenerate subspaces where k is odd.
   - M acts on k-dimensional non-degenerate subspaces U of V for k even, and where U is of plus type.
   - M acts on k-dimensional non-degenerate subspaces U of V for k even, and where U is of minus type.
   - M acts on one-dimensional non-singular subspaces.
6. $T = \mathrm{P}\Omega_d^-(q)$
   - M acts on k-dimensional singular subspaces.
   - M acts on k-dimensional non-degenerate subspaces where k is odd.
   - M acts on k-dimensional non-degenerate subspaces $U < V$ for k even, and where U is of plus type.
   - M acts on k-dimensional non-degenerate subspaces $U < V$ for k even, and where U is of minus type.
   - M acts on one-dimensional non-singular subspaces.

For a given q, d, and k, all subgroups T with an action given by one of the bullet points in the list above are permutation isomorphic. Note that some of these only occur for k even, others for k odd. Similarly, some groups only occur for d even, others for d odd. For a given q, d, k, we get at most one conjugacy class in S_n of subgroups $M < G$ for each point in the list above. These conjugacy classes may split over A_n. We wish to bound the order of M, and the number of conjugacy classes of such subgroups in terms of n. We will use the following two lemmas.

Lemma 4.7.1. *Let T be a simple classical group of degree d, defined over a field of order q. Let H be an almost simple group with socle T and let it act primitively on orbits of subspaces, or pairs of subspaces. Then the length n of the orbit is greater than or equal to* $\max\{q^{d-2}, q\}$.

Proof. So H_α is maximal in H and is the stabiliser of a subspace (or pair of subspaces), then $n = [H : H_\alpha] \geq \rho(T)$, where $\rho(T)$ is the minimal degree of a permutation representation of T. By Theorem 2.2.42, if $T \neq \mathrm{PSL}_2(9)$, then $\rho(T) \geq \max\{q^{d-2}, q\}$.

Now consider $T = \mathrm{PSL}_2(9)$, that is, $d = 2$ and $q = 9$. Then H may act on one-dimensional subspaces of V. In this case n is the number of one dimensional subspaces of V which is equal to $(q^2-1)/(q-1) = q+1$. This comes from counting the possible number of basis vectors for the subspace. So for $T = \mathrm{PSL}_2(9)$, $n \geq \max\{q^{d-2}, q\}$. □

Lemma 4.7.2. *Let T be a simple classical group of dimension d, defined over a field of order q. Then $|\mathrm{Aut}(T)| \leq q^{d^2}$.*

Proof. We consider each simple classical group in turn. The orders of simple classical groups are given in Section 2.2.1 and the orders of the corresponding outer automorphism groups are given in Table 2.9.

First let $T = \mathrm{PSL}_d(q)$. Then

$$\begin{aligned} |\mathrm{Aut}(T)| &\leq 2(\log_p q) q^{d(d-1)/2} \prod_{i=2}^{d} (q^i - 1) \\ &\leq q \times q^{d(d-1)/2} \prod_{i=2}^{d} q^i \\ &\leq q^{d^2}. \end{aligned}$$

Next consider $T = \mathrm{PSp}_d(q)$ where $d = 2m$. Then,

$$\begin{aligned} |\mathrm{Aut}(T)| &\leq (2\log_p q) q^{m^2} \prod_{i=1}^{m} (q^{2i} - 1) \\ &\leq q^{m^2+1} \prod_{i=1}^{m} q^{2i} \\ &\leq q^{2m^2+m+1} \\ &\leq q^{d^2}. \end{aligned}$$

Now suppose $T = \mathrm{PSU}_d(q)$. Then,

$$\begin{aligned} |\mathrm{Aut}(T)| &\leq 2(\log_p q) q^{d(d-1)/2} \prod_{i=2}^{d} (q^i - (-1)^i) \\ &\leq q \times q^{d(d-1)/2} \prod_{i=1}^{d} q^i \\ &\leq q^{d^2}. \end{aligned}$$

Let $T = \Omega_d(q)$ for $d = 2m+1$, then

$$\begin{aligned} |\mathrm{Aut}(T)| &\leq (\log_p q) q^{m^2} \prod_{i=1}^{m} (q^{2i}-1) \\ &\leq q^{m^2+1} \prod_{i=1}^{m} q^{2i} \\ &\leq q^{2m^2+m+1} \\ &\leq q^{d^2}. \end{aligned}$$

Finally let $T = \mathrm{P}\Omega_d^{\pm}(q)$ for $d = 2m$, then,

$$\begin{aligned} |\mathrm{Aut}(T)| &\leq 6(\log_p q) q^{m(m-1)} (q^m \mp 1) \prod_{i=1}^{m-1} (q^{2i}-1) \\ &\leq (6 \log q) q^{m(m-1)} (q^m + 1) \prod_{i=1}^{m-1} q^{2i} \\ &\leq q^{4m^2} \\ &\leq q^{d^2}. \end{aligned}$$

□

Lemma 4.7.3. *Let $\mathcal{M}$ be a set of conjugacy class representatives for maximal subgroups of $G = A_n$ or S_n, where M is an almost simple classical group acting on orbits of subspaces of the natural module, or pairs of subspaces of complementary dimensions (if $\mathrm{Soc}(M) = \mathrm{PSL}_d(q)$). Then*

$$\sum_{M \in \mathcal{M}} \frac{1}{[G:M]} \leq \frac{52(\log n + 1)(\log n + 2) n^{\log n + 9}}{n!}.$$

Proof. Let M be an almost simple classical group of dimension d defined over a field of order q, and let V be the corresponding natural module. Let $S = \mathrm{Soc}(M)$. Then M acts on subspaces of V of order k, or pairs of subspaces of complementary dimensions. As described at the start of this section for any given q, d, k, there are at most 13 different possibilities for M together with its action on subspaces. The conjugacy classes in S_n are determined by choosing q, d, k, the isomorphism type of S, together with its action on subspaces. By Lemma 4.0.3 these conjugacy classes may split over A_n. Then the number of conjugacy classes of maximal subgroups in $\mathcal{M}$ is bounded above by 26 times the number of possibilities for q, d, k.

By Lemma 4.7.1, $q \leq n$, $q^{d-2} \leq n$, and $d \leq \log n + 2$. As $k < d$, then $k \leq \log n + 1$. Then for $M \in \mathcal{M}$ we use Lemma 4.7.2 to bound the order:

$$|M| \leq q^{d^2} = q^4 (q^{d-2})^{d+2} \leq n^4 n^{\log n + 4} \leq n^{\log n + 8}.$$

Then

$$\begin{aligned}\sum_{M\in\mathcal{M}}\frac{1}{[G:M]} &\leq \frac{26n(\log n+1)(\log n+2)n^{\log n+8}}{n!/2}\\ &\leq \frac{52(\log n+1)(\log n+2)n^{\log n+9}}{n!}.\end{aligned}$$

□

4.8 Maximal subgroups of order at most n^c

Suppose that M is a maximal almost simple subgroup of $G = A_n$ or S_n such that $|M| \leq n^c$, for $c = 6.077948094$. The number of possibilities for M is bounded above by the number of possible simple subgroups $T \leq G$. A simple subgroup $T \leq G$ embeds in S_n if and only if T has a faithful permutation representation of degree n. As permutation representations of T of degree n correspond to conjugacy classes of subgroups of T of index n, we estimate the number of permutation representations using the following proposition.

Proposition 4.8.1 ([80, Proposition 4.1])**.** *Let H be a finite group. The number of subgroups of index n in H is less than or equal to $|H|^{2\log n}$.*

Note that in the following lemma we will be bounding the number of maximal subgroups M, not the number of conjugacy classes as in previous cases.

Lemma 4.8.2. *Let $G = A_n$ or S_n, and let $c = 6.077948094$. Then*

$$\sum_{\substack{M<_{\max}G\\ M \text{ almost simple}\\ |M|\leq n^c}}\frac{1}{[G:M]^2} \leq \frac{4n^{2c\log n+3c}}{(n!)^2}.$$

Proof. Let k denote the number of almost simple maximal subgroups of order at most n^c. Then

$$\begin{aligned}\sum_{\substack{M<_{\max}G\\ M \text{ almost simple}\\ |M|\leq n^c}}\frac{1}{[G:M]^2} &\leq \frac{k|M|^2}{|A_n|^2}\\ &\leq \frac{4kn^{2c}}{(n!)^2}.\end{aligned}$$

For each simple group T in S_n there is at most one maximal almost simple subgroup M with socle T, namely $M = N_G(T)$. To find an upper bound on

the number of maximal subgroups M in G such that $|M| \leq n^c$ it suffices to count the number of simple subgroups $T \leq G$ such that $|T| \leq n^c$.

The number of ways of embedding T into G (that is, the number of subgroups of G which are isomorphic to T) is at most the number of ways of embedding T into S_n. This is equal to the number of faithful representations of T of degree n. Permutation representations of T of index n correspond to subgroups of T of degree n. Then the number of ways of embedding T into G is at most the number of subgroups $H < T$ where $[T : H] = n$. This is of course bounded by the number of subgroups H of T of index n, and by Proposition 4.8.1, the number of isomorphic copies of a simple group T embedded in G, where $|T| \leq n^c$, is at most $n^{2c \log n}$.

Up to isomorphism, the number of simple groups of order at most n^c is at most n^c as by the Classification of Finite Simple Groups there are at most 2 simple groups of any given even order. Then

$$k \leq n^{c+2c \log n}$$

and so

$$\sum_{\substack{M <_{\max} G \\ M \text{ almost simple} \\ |M| \leq n^c}} \frac{1}{[G : M]^2} \leq \frac{4n^{2c \log n + 3c}}{(n!)^2}.$$

□

4.9 Estimate for $P_{G,A_n}(2)$, and proof of theorem

First we combine the sums from the previous sections to estimate the probability $P_{G,A_n}(2)$, for $G = A_n$ or S_n.

Theorem 4.9.1. *Let $G = A_n$ or S_n. Then*

$$\begin{aligned} P_{G,A_n}(2) \geq 1 - \Bigg(& \frac{1}{n} + \frac{3}{2n(n-1)} + \frac{3}{(n-1)(n-2)} + \frac{\sqrt{n}}{2^{n/4-1}} \\ & + \frac{4}{(n - \lfloor \log n \rfloor - 1)!} + \frac{8n(\log n)(\lfloor \log_{60} n \rfloor + 1)!}{(n-1)!} + \frac{1}{n^{n/3}} \\ & + \frac{4(\sqrt{2n} - 3)(\lfloor \sqrt{2n} \rfloor + 1)!}{n!} + \frac{32(\log n)^2(\lfloor 4 \log n \rfloor)!}{n!} \\ & + \frac{52(\log n + 1)(\log n + 2)n^{\log n + 9}}{n!} + \frac{4n^{13 \log n + 19}}{(n!)^2} \Bigg). \end{aligned}$$

If $n \geq 64$, then $P_{G,A_n}(2) \geq 0.979$.

Proof. Theorem 2.1.24 and Theorem 4.0.4, give the possibilities for transitive maximal subgroups of G. Then Lemmas 4.3.1, 4.4.1, 4.5.1, 4.6.2, 4.6.4, 4.7.3 and 4.8.2 bound the sum,

$$\sum_{\substack{M<_{\max}G \\ M \text{ transitive} \\ M\neq A_n}} \frac{1}{[G:M]^2} \leq \frac{\sqrt{n}}{2^{n/4-1}} + \frac{4}{(n-\lfloor \log n\rfloor -1)!} + \frac{8n(\log n)(\lfloor \log_{60} n\rfloor +1)!}{(n-1)!} + \frac{1}{n^{n/3}} + \frac{4(\sqrt{2n}-3)(\lfloor \sqrt{2n}\rfloor +1)!}{n!} + \frac{32(\log n)^2(\lfloor 4\log n\rfloor)!}{n!} + \frac{52(\log n+1)(\log n+2)n^{\log n+9}}{n!} + \frac{4n^{13\log n+19}}{(n!)^2}.$$

By Lemma 4.0.2

$$P_{G,A_n}(2) \geq 1 - Q_1(G) - \sum_{\substack{M<_{\max}G \\ M \text{ transitive} \\ M\neq A_n}} \frac{1}{[G:M]^2}$$

where $Q_1(G)$ is as defined in 4.0.2. Lemma 4.2.1 bounds $Q_1(G)$, and this gives bound on $P_{G,A_n}(2)$. This bound is increasing with increasing n, and so $P_{G,A_n}(2) \geq 0.979$ holds for $n \geq 64$. □

First we prove the following preliminary result to show that all but finitely many almost simple G with socle A_n satisfy $P_{G,A_n}(2) \geq 0.927$. This will be useful for bounding $P_{G,A_n}(3)$ in Chapter 8.

Lemma 4.9.2. *Let G be an almost simple group with socle A_n. Then $P_{G,A_n}(2) < 0.927$ implies $n \leq 16$.*

Proof. By the previous result, $P_{G,A_n}(2) \geq 0.927$ for $n \geq 64$. Maximal subgroup information for A_n and S_n for $n \leq 63$ is available in GAP [28]. Then we may estimate $P_{G,A_n}(2)$ in GAP using Lemma 3.2.6. These estimates show that for $17 \leq n \leq 63$, $P_{G,A_n}(2) \geq 0.927$ as required. □

We cannot determine precisely which values of n give $P_{G,A_n}(2) \leq 0.927$. We have only been able to calcuate $P_{G,G_0}(2)$ exactly for $n \leq 13$ as tables of marks are available in GAP for these groups [74, 28]. Without the tables of marks, the exact calculation takes too long. For $14 \leq n \leq 16$, we may calculate a lower bound for $P_{G,A_n}(2)$. This is enough to show that the probability is at least 0.9, but not enough to show that the probability is at least 0.927.

Thus we may complete the proof of Theorem 4.0.1, and bound $P_{G,A_n}(2)$ below.

Proof of Theorem 4.0.1. Theorem 4.9.1 estimates the probability, and shows that when $n \geq 64$, then $P_{G,A_n}(2) \geq 0.979$. For $14 \leq n \leq 63$, computational estimates show that $P_{G,A_n}(2) > 0.912$. Finally for $5 \leq n \leq 13$, exact values for $P_{G,A_n}(2)$ have been calculated (Table 4.1). These results show that $P_{G,A_n}(2) > 0.9$ if and only if $n \geq 12$, and in all cases $P_{G,A_n}(2) \geq 53/90$, with equality if and only if $G = S_6$ or A_6. □

Chapter 5

The probability of generating a simple classical group

In this chapter let G_0 be a simple classical group, and let $G_0 \leq G \leq \mathrm{Aut}(G_0)$. Recall from Theorem 3.1.6 that $d(G) = 2$ or 3, and $d(G) = 3$ implies that $G_0 = \mathrm{PSL}_n(p^f)$ for $n \geq 4$ even, p odd and f even, or $G_0 = \mathrm{P}\Omega_n^+(p^f)$ for $n \geq 8$, p odd and f even. In this chapter we are interested in $P_{G,G_0}(2)$, and so we consider those G which may be generated by 2 elements. In this chapter we prove the following.

Theorem 5.0.1. *Let G be an almost simple group with socle G_0, where G_0 is a classical group which is not isomorphic to an alternating group. Suppose that G can be generated by 2 elements. Then $P_{G,G_0}(2) \geq 19/28 > 0.678$. Additionally $P_{G,G_0}(2) \geq 0.927$ unless G is isomorphic to one of the 24 groups listed in Table 5.1.*

Alternating groups isomorphic to classical groups are: $A_5 \cong \mathrm{PSL}_2(4) \cong \mathrm{PSL}_2(5)$, $A_6 \cong \mathrm{PSL}_2(9) \cong \mathrm{Sp}_4(2)'$, and $A_8 \cong \mathrm{PSL}_4(2)$. We exclude almost simple classical groups with these socles as they have been considered in the previous chapter.

We use Lemma 3.2.6 to estimate the probability,

$$P_{G,G_0}(2) \geq 1 - \sum_{M \in \mathcal{M}} \frac{1}{[G : M]},$$

where $\mathcal{M}$ is a set of conjugacy class representatives for maximal subgroups of G not containing G_0.

The probability of generating a classical group with two elements is estimated in [40]. The main theorem of [40] is the following.

Theorem 5.0.2 ([40])**.** *Let G_0 denote a finite simple classical group, and let $G_0 \leq G \leq \mathrm{Aut}(G_0)$. Let $P(G)$ be the probability that 2 randomly chosen elements of G generate a group containing G_0, then $P(G) \to 1$ as $|G| \to \infty$.*

G	$G_0 = \mathrm{Soc}(G)$	$P_{G,G_0}(2)$	$P_{G,G_0}(2)$
$\mathrm{PSL}_2(7) \cong \mathrm{PSL}_3(2)$	$\mathrm{PSL}_2(7)$	19/28	0.678
$\mathrm{PSL}_2(11)$	$\mathrm{PSL}_2(11)$	127/165	0.769
$\mathrm{PSL}_2(7).2 \cong \mathrm{PSL}_3(2).2$	$\mathrm{PSL}_2(7)$	23/28	0.821
$\mathrm{PSL}_2(8)$	$\mathrm{PSL}_2(8)$	71/84	0.845
$\mathrm{P\Gamma L}_2(8)$	$\mathrm{PSL}_2(8)$	71/84	0.845
$\mathrm{PSL}_3(3)$	$\mathrm{PSL}_3(3)$	101/117	0.863
$\mathrm{PSL}_3(4)$	$\mathrm{PSL}_3(4)$	121/140	0.864
$\mathrm{PSL}_2(11).2$	$\mathrm{PSL}_2(11)$	146/165	0.884
$\mathrm{PSU}_4(2) \cong \mathrm{PSp}_4(3)$	$\mathrm{PSU}_4(2)$	767/864	0.887
$\mathrm{PSU}_4(2).2$	$\mathrm{PSU}_4(2)$	767/864	0.887
$\mathrm{PSL}_3(4).2_2$	$\mathrm{PSL}_3(4)$	4519/5040	0.896
$\mathrm{PSL}_2(13)$	$\mathrm{PSL}_2(13)$	165/182	0.906
$\mathrm{PGL}_2(13)$	$\mathrm{PSL}_2(13)$	165/182	0.906
$\mathrm{PSp}_6(2)$	$\mathrm{PSp}_6(2)$	219703/241920	0.908
$\mathrm{PSL}_3(4).2_1$	$\mathrm{PSL}_3(4)$	1541/1680	0.917
$\mathrm{P\Gamma L}_3(4)$	$\mathrm{PSL}_3(4)$	3067/3360	0.912
$\mathrm{PGL}_3(4)$	$\mathrm{PSL}_3(4)$	3067/3360	0.912
$\mathrm{PSU}_3(3).3$	$\mathrm{PSU}_3(3)$	11/12	0.916
$\mathrm{PSL}_2(19)$	$\mathrm{PSL}_2(19)$	157/171	0.918
$\mathrm{PSL}_2(16)$	$\mathrm{PSL}_2(16)$	313/340	0.920
$\mathrm{PSL}_2(16).2$	$\mathrm{PSL}_2(16)$	313/340	0.920
$\mathrm{P\Gamma L}_2(16)$	$\mathrm{PSL}_2(16)$	313/340	0.920
$\mathrm{PSU}_3(3)$	$\mathrm{PSU}_3(3)$	58/63	0.920
$\mathrm{PSL}_2(17)$	$\mathrm{PSL}_2(17)$	283/306	0.924

Table 5.1: Almost simple groups G with $0.678 < P_{G,G_0}(2) < 0.927$

This proof uses the bound

$$P(G) \geq 1 - \sum_{L \in \mathcal{L}} \frac{1}{[G:L]},$$

where $\mathcal{L}$ is a set of conjugacy class representatives for subgroups L of G which are maximal with respect to not containing G_0. As $\mathcal{M} \subseteq \mathcal{L}$ then we might hope that these bounds from [40] may be useful for us. The bounds on

$$\sum_{L \in \mathcal{L}} \frac{1}{[G:L]}$$

from [40] are estimated in the following manner. Subgroups L are described by Aschbacher's Theorem, and comprise 8 classes $\mathcal{C}_1$ to $\mathcal{C}_8$ of geometric maximal subgroups, and a class $\mathcal{S}$ of almost simple subgroups. The number of conjugacy classes of geometric maximal subgroups is known, and easily

bounded, and $[G : L]$ is bounded below by the minimal degree of a permutation representation of G_0. Almost simple maximal subgroups have a much smaller order [51] and so we have a better bound on their index. The number of such subgroups is estimated by estimating the possible number of representations of $\tilde{S}$, for simple subgroups S of G_0. If $G_0 = \mathrm{PSL}_n(q)$, the estimates in [40] are good enough to show $P_{G,G_0}(2) \geq 53/90$ for $n \geq 10$, otherwise these estimates are good enough if the dimension n of G is greater than 20 (although for small values of n and q the bounds may need to be tightened slightly, or checked computationally). We would like to find better bounds, in particular ones that are good enough to show $P_{G,G_0}(2) \geq 53/90$ for all values of n, and preferably bounds that allow us to show that the probability is greater than 0.9 (or better still, $P_{G,G_0}(2) \geq 0.927$ to help with bounding $P_{G,G_0}(3)$) for all but finitely many groups.

The idea of our proof is similar, we also use Aschbacher's Theorem to estimate the number of maximal subgroups of G, and estimate the index of maximal subgroups using the smallest degree of a permutation representation of G_0. Again we have a better bound on the index of maximal subgroups in $\mathcal{S}$ using [51] to bound their order. We have improved bounds on the number of conjugacy classes of maximal subgroups from [44] and [33], and in particular [33] gives much better bounds for the number of conjugacy classes of almost simple maximal subgroups. The bounds we obtain are good enough to show $P_{G,G_0}(2) \geq 0.927$ when the dimension n of G is greater than 12 (and in many cases, for smaller n). For classical groups in dimension at most 12, full maximal subgroup information is available in [10], and so it is easy to bound the probability in these cases. We also use GAP [28] and Magma [8] to calculate either the exact probability, or lower bounds, when $|G|$ is small. In most cases we may also show $P_{G,G_0}(2) \geq 0.927$, which will be useful in the proof of a lower bound for $P_{G,G_0}(3)$.

5.1 Classical groups in large dimensions

We may estimate the number of conjugacy classes of maximal subgroups of an almost simple classical group G using the following.

Theorem 5.1.1 ([33, Theorem 1.1])**.** *Let G be a finite almost simple group with socle G_0 a classical group of dimension n over the field $\mathbb{F}_q$. Let $m(G)$ denote the number of conjugacy classes of maximal subgroups of G not containing the socle. Then*

$$m(G) < 2n^{5.2} + n \log\log q.$$

Next we calculate the index of maximal subgroups in G. By Lemma 3.2.7, $[G : M] = [G_0 : G_0 \cap M]$, and this may be bounded below by the minimum degree of a permutation representation of G_0. These degrees are given in Theorem 2.2.42.

Then if $\mathcal{M}$ denotes a set of conjugacy class representatives for maximal subgroups of G not containing G_0 then,

$$\sum_{M \in \mathcal{M}} \frac{1}{[G:M]} \leq \frac{m(G)}{\rho(G_0)}.$$

Hence we have the following lower bounds on

$$P_{G,G_0}(2) \geq 1 - \sum_{M \in \mathcal{M}} \frac{1}{[G:M]} \geq 1 - \frac{m(G)}{\rho(G_0)}.$$

Theorem 5.1.1 bounds $m(G)$ and Theorem 2.2.42 bounds $\rho(G_0)$, and so Theorems 5.1.2 – 5.1.7 which bound $P_{G,G_0}(2)$ for each family of classical groups follow immediately.

Due to isomorphisms between classical groups of small dimensions, we only have to consider dimension $n \geq 3$ in the unitary case, $n \geq 4$ in the symplectic case, $n \geq 7$ in the orthogonal case. We have the additional restrictions of $n \geq 3$ and $n \geq 5$ in the linear and unitary cases respectively to avoid considering as many cases from Theorem 2.2.42. For small n the bounds obtained using this method are not good enough to bound the probability anyway. We will consider bounds for $\mathrm{PSL}_2(q)$, $\mathrm{PSU}_3(q)$ and $\mathrm{PSU}_4(q)$ in Section 5.2 as we have full lists of maximal subgroups for the corresponding quasisimple groups in these cases.

Theorem 5.1.2. *Let $G_0 = \mathrm{PSL}_n(q)$ where $n \geq 3$, $G_0 \neq \mathrm{PSL}_4(2)$, and let $G_0 \leq G \leq \mathrm{Aut}(G_0)$ where G can be generated by 2 elements. Then*

$$P_{G,G_0}(2) \geq 1 - \frac{(2n^{5.2} + n \log\log q)(q-1)}{(q^n - 1)}$$

and if $n \geq 30$, then $P_{G,G_0}(2) > 0.9$.

Theorem 5.1.3. *Let $G_0 = \mathrm{PSp}_n(q)$ where $n \geq 4$, and let $G_0 \leq G \leq \mathrm{Aut}(G_0)$.*

1. *If $q = 2$ and $n \geq 6$ then*

$$P_{G,G_0}(2) \geq 1 - \frac{n^{5.2}}{2^{(n-1)/2}(2^{n/2} - 1)},$$

   and if $n \geq 32$, then $P_{G,G_0}(2) > 0.9$.

2. *If $q \neq 2$, then*

$$P_{G,G_0}(2) \geq 1 - \frac{(2n^{5.2} + n \log\log q)(q-1)}{(q^n - 1)},$$

   and if $n \geq 17$, then $P_{G,G_0}(2) > 0.9$.

Theorem 5.1.4. *Let $G_0 = \mathrm{PSU}_n(q)$ where $n \geq 5$, and let $G_0 \leq G \leq \mathrm{Aut}(G_0)$.*

1. *If n is even and $q = 2$, then*

$$P_{G,G_0}(2) \geq 1 - \frac{3n^{5.2}}{2^{n-2}(2^n - 1)},$$

and if $n \geq 14$, then $P_{G,G_0}(2) > 0.9$.

2. *If $(n, q) \neq (2m, 2)$, then*

$$P_{G,G_0}(2) \geq 1 - \frac{(2n^{5.2} + n \log\log q)(q^2 - 1)}{(q^n - (-1)^n)(q^{n-1} - (-1)^{n-1})},$$

and if $n \geq 14$, then $P_{G,G_0}(2) > 0.9$.

Theorem 5.1.5. *Let $G_0 = \Omega_n(q)$ where $n \geq 7$ and nq is odd, and let $G_0 \leq G \leq \mathrm{Aut}(G_0)$.*

1. *If $q = 3$, then*

$$P_{G,G_0}(2) \geq 1 - \frac{4n^{5.2} + 2n \log\log 3}{3^{(n-1)/2}(3^{(n-1)/2} - 1)},$$

and if $n \geq 19$, then $P_{G,G_0}(2) > 0.9$.

2. *If $q \geq 5$, then*

$$P_{G,G_0}(2) \geq 1 - \frac{(2n^{5.2} + n \log\log q)(q - 1)}{(q^{n-1} - 1)},$$

and if $n \geq 13$, then $P_{G,G_0}(2) > 0.9$.

Theorem 5.1.6. *Let $G_0 = \mathrm{P}\Omega_n^+(q)$ where $n \geq 8$, and let $G_0 \leq G \leq \mathrm{Aut}(G_0)$, where G can be generated by 2 elements.*

1. *If $q = 2$, then*

$$P_{G,G_0}(2) \geq 1 - \frac{n^{5.2}}{2^{(n-1)/2}(2^{n/2} - 1)},$$

and if $n \geq 32$, then $P_{G,G_0}(2) > 0.9$.

2. *If $q = 3$, then*

$$P_{G,G_0}(2) \geq 1 - \frac{4n^{5.2} + 2n \log\log 3}{3^{n/2-1}(3^{n/2} - 1)},$$

and if $n \geq 20$, then $P_{G,G_0}(2) > 0.9$.

3. If $q \geq 4$, then

$$P_{G,G_0}(2) \geq 1 - \frac{(2n^{5.2} + n\log\log q)(q-1)}{(q^{n/2}-1)(q^{n/2-1}+1)},$$

and if $n \geq 14$, then $P_{G,G_0}(2) > 0.9$.

Theorem 5.1.7. *Let $G_0 = \mathrm{P}\Omega_n^-(q)$ where $n \geq 8$, and let $G_0 \leq G \leq \mathrm{Aut}(G_0)$. Then*

$$P_{G,G_0}(2) \geq 1 - \frac{(2n^{5.2} + n\log\log q)(q-1)}{(q^{n/2}+1)(q^{n/2-1}-1)},$$

and if $n \geq 32$, then $P_{G,G_0}(2) > 0.9$.

These bounds are increasing with increasing n and q. Whilst these results hold for almost all values of n, they are only useful for 'large' n (depending on G_0) as indicated. We can also show $P_{G,G_0}(2) > 0.9$ for some smaller values of n, but we must take q to be large enough. When $n \leq 12$ we have full maximal subgroup information for $\mathrm{SL}_n(q)$, $\mathrm{Sp}_n(q)$, $\mathrm{SU}_n(q)$, $\Omega_n(q)$ and $\Omega_n^{\pm}(q)$ from [10] and in the next section we see how this allows us to estimate the probability for generating the corresponding projective groups. It remains to improve these bounds, in particular we need bounds that are useful for $n \geq 13$ and all values of q.

Recall maximal subgroups of G fall into one of 9 classes: geometric maximal subgroups $\mathcal{C}_1$ – $\mathcal{C}_8$, and almost simple subgroups $\mathcal{S}$. Recall, $\mathcal{C}_G$ denotes the set of geometric maximal subgroups.

Next we define a subset $\mathcal{E}$ of $\mathcal{S}$ as in [51, Section 4].

Definition 5.1.8. Let $\mathcal{E}$ denote the subgroups H in $\mathcal{S}$ which are of the form A_{n+1}, S_{n+1}, A_{n+2} or S_{n+2}, and which are embedded as in [51, Section 4]. We denote the set $\mathcal{S} \setminus \mathcal{E}$ by $\mathcal{S}'$.

By [51], we only get subgroups in $\mathcal{E}$ when G is orthogonal or symplectic. We get at most 2 inequivalent faithful representations of each of S_{n+1} and S_{n+2}, and at most one of A_{n+1} and A_{n+2}.

Theorem 5.1.9 ([51, Theorem 4.1])**.** *Let G_0 be a simple classical group with natural projective module V of dimension n over $\mathbb{F}_q$, and let G be a group such that $G_0 \leq G \leq \mathrm{Aut}(G_0)$. Let H be a maximal subgroup of G such that $G = HG_0$. Then one of the following holds:*

1. *$H \in \mathcal{C}_G$;*
2. *$H \in \mathcal{E}$;*
3. *$|H| \leq q^{3n}$.*

Note that in the case $G_0 = \mathrm{PSU}_n(q)$ the natural module is defined over the field $\mathbb{F}_{q^2}$.

Lemma 5.1.10. *Let G_0 be a simple classical group, and let G be an almost simple subgroup with socle G_0. Let $m_{\mathcal{G}}(G)$ be the number of conjugacy classes of geometric maximal subgroups of G.*

1. *If $G_0 = \mathrm{PSL}_n(q)$ for $n \geq 2$, then $m_{\mathcal{G}}(G) \leq 6n + \frac{n}{3}\log n + n\log\log q$.*
2. *If $G_0 = \mathrm{PSp}_n(q)$ for $n \geq 4$, then $m_{\mathcal{G}}(G) \leq 2n + 2\log n + 2\log\log q$.*
3. *If $G_0 = \mathrm{PSU}_n(q)$ for $n \geq 3$, then $m_{\mathcal{G}}(G) \leq 5n + \frac{n}{3}\log n + n\log\log q$.*
4. *If $G_0 = \Omega_n(3)$ for $n \geq 7$, then $m_{\mathcal{G}}(G) \leq 3n + 2\log n$.*
5. *If $G_0 = \Omega_n(q)$ for $n \geq 7$, where nq is odd, then $m_{\mathcal{G}}(G) \leq 3n + 2\log n + 2\log\log q$.*
6. *If $G_0 = \mathrm{P}\Omega_n^+(2)$ for $n \geq 8$, then $m_{\mathcal{G}}(G) \leq 2n + 2\log n$.*
7. *If $G_0 = \mathrm{P}\Omega_n^+(3)$ for $n \geq 8$, then $m_{\mathcal{G}}(G) \leq 8n + 9\log n$.*
8. *If $G_0 = \mathrm{P}\Omega_n^+(q)$ for $n \geq 8$, then $m_{\mathcal{G}}(G) \leq 8n + 9\log n + 4\log\log q$.*
9. *If $G_0 = \mathrm{P}\Omega_n^-(q)$ for $n \geq 8$, then $m_{\mathcal{G}}(G) \leq 3n + \log n + \log\log q$.*

Proof. Let M be a geometric maximal subgroup of some almost simple group with socle G_0. Then the number of conjugacy classes of subgroups $M \cap G_0$ is given in [44, Tables 3.5.A – 3.5.G]. Conjugacy classes of maximal subgroups may split over G_0, so the number of conjugacy classes of subgroups in G_0 is an upper bound on the number of conjugacy classes of maximal subgroups of G. □

Next we bound the number of conjugacy classes of maximal subgroups in $\mathcal{E}$. Recall we only get maximal subgroups of this form when G is symplectic or orthogonal. Let $\rho : S_c \to \mathrm{GL}_n(F)$ be a faithful representation of S_c. Define the map $\sigma : S_c \to \mathrm{GL}_n(F)$ by

$$g\sigma = \begin{cases} g\rho & \text{if } g \text{ even} \\ -g\rho & \text{if } g \text{ odd} \end{cases}$$

Then σ is another inequivalent faithful representation of S_c. Both σ and ρ yield conjugate subgroups of the projective group. So, if we have two inequivalent faithful representations of S_c, they correspond to one projective representation.

Lemma 5.1.11. *Let G_0 be a simple classical group, let $G_0 \leq G \leq \mathrm{Aut}(G_0)$, and let $m_{\mathcal{E}}(G)$ denote a set of conjugacy class representatives for maximal subgroups of G lying in $\mathcal{E}$. Then we may bound $m_{\mathcal{E}}(G)$ as follows.*

1. *If* $G_0 = \mathrm{PSp}_n(q)$ *for* $n \geq 4$, *then* $m_{\mathcal{E}}(G) \leq 4$.

2. *If* $G_0 = \Omega_n(q)$ *for* $n \geq 7$, *then* $m_{\mathcal{E}}(G) \leq 4$.

3. *If* $G_0 = \mathrm{P}\Omega_n^{\pm}(q)$ *for* $n \geq 8$, *then* $m_{\mathcal{E}}(G) \leq 16$.

Proof. By the observation above we get at most 1 inequivalent faithful projective representation of either S_{n+1} or A_{n+1}, and 1 of either S_{n+2} or A_{n+2} in $\mathcal{E}$. Equivalent representations are conjugate in the corresponding projective conformal group $C = \mathrm{PCSp}_n(q)$ or $\mathrm{PCGO}_n^{\epsilon}(q)$ and so we multiply by $[C : G_0]$ to get an upper bound on the number of conjugacy classes of maximal subgroups (in $\mathcal{E}$) lying in G. From Section 2.2.1, $[C : G_0] \leq 2$ when $G_0 = \mathrm{PSp}_n(q)$ or $\Omega_n(q)$, and $[C : G_0] \leq 8$ when $G_0 = \mathrm{P}\Omega_n^{\pm}(q)$. The result follows. □

We bound $P_{G,G_0}(2)$ in the following 6 theorems. These will be proved together at the end of Theorem 5.1.17.

Theorem 5.1.12. *Let* G *be an almost simple group with socle* $G_0 = \mathrm{PSL}_n(q)$ *for* $n \geq 3$. *Suppose* G *can be generated by two elements. Then*

$$\begin{aligned} P_{G,G_0}(2) \geq 1 \quad &- \quad \frac{(18n + n\log n + 3n\log\log q)(q-1)}{3(q^n-1)} \\ &- \quad \frac{(2n^{5.2} + n\log\log q)(q-1)}{q^{n(n-7)/2}\prod_{i=2}^{n}(q^i-1)}. \end{aligned}$$

If $n \geq 12$, *if* $n \geq 7$ *and* $q \geq 3$, *if* $n \geq 6$ *and* $q \geq 4$, *or if* $n \geq 5$ *and* $q \geq 5$, *then* $P_{G,G_0}(2) \geq 0.930$.

Theorem 5.1.13. *Let* G *be an almost simple group with socle* $G_0 = \mathrm{PSp}_n(q)$ *for* $n \geq 4$.

1. *If* $G_0 = \mathrm{Sp}_n(2)$ *for* $n \geq 6$, *then*

$$P_{G,G_0}(2) \geq 1 - \frac{n + \log n + 2}{2^{(n-1)/2}(2^{n/2}-1)} - \frac{2n^{5.2}}{2^{n(n-12)/4}\prod_{i=1}^{n/2}(2^{2i}-1)}.$$

2. *If* $G_0 = \mathrm{PSp}_n(q)$ *for* $n \geq 4$ *and* $q \geq 3$, $G_0 \neq \mathrm{PSp}_4(3)$, *then*

$$\begin{aligned} P_{G,G_0}(2) \geq 1 \quad &- \quad \frac{(2n + 2\log n + 2\log\log q + 4)(q-1)}{(q^n-1)} \\ &- \quad \frac{(4n^{5.2} + 2n\log\log q)}{q^{n(n-12)/4}\prod_{i=1}^{n/2}(q^{2i}-1)}. \end{aligned}$$

If $n \geq 10$, *then* $P_{G,G_0}(2) \geq 0.938$.

Theorem 5.1.14. *Let G be an almost simple group with socle $G_0 = \mathrm{PSU}_n(q)$ for $n \geq 5$.*

1. *If $G_0 = \mathrm{PSU}_n(2)$ for $n \geq 6$ and n even, then*

$$P_{G,G_0}(2) \geq 1 - \frac{15n + n\log n}{2^{n-1}(2^n - 1)} - \frac{2n^{5.2}}{2^{n(n-13)/2}\prod_{i=2}^{n}(2^i - (-1)^i)}.$$

2. *If $G_0 = \mathrm{PSU}_n(q)$ for $n \geq 5$, and $(n,q) \neq (2m,2)$, then*

$$\begin{aligned} P_{G,G_0}(2) \geq 1 \quad &- \quad \frac{(15n + n\log n + 3n\log\log q)(q^2-1)}{3(q^n - (-1)^n)(q^{n-1} - (-1)^{n-1})} \\ &+ \quad \frac{(2n^{5.2} + n\log\log q)(q+1)}{q^{n(n-13)/2}\prod_{i=2}^{n}(q^i - (-1)^i)}. \end{aligned}$$

If $n \geq 9$, if $n \geq 8$ and $q \geq 3$, or if $n \geq 7$ and $q \geq 16$, then $P_{G,G_0}(2) \geq 0.949$.

Theorem 5.1.15. *Let G be an almost simple group with socle $G_0 = \Omega_n(q)$ for $n \geq 7$.*

1. *If $G_0 = \Omega_n(3)$ for $n \geq 7$, then*

$$P_{G,G_0}(2) \geq 1 - \frac{6n + 4\log n + 8}{3^{(n-1)/2}(3^{(n-1)/2} - 1)} - \frac{4n^{5.2} + 2n\log\log 3}{3^{(n^2-14n+1)/4}\prod_{i=1}^{(n-1)/2}(3^{2i} - 1)}.$$

2. *If $G_0 = \Omega_n(q)$ for $n \geq 7$ and $q \geq 5$, then*

$$\begin{aligned} P_{G,G_0}(2) \geq 1 \quad &- \quad \frac{(3n + 2\log n + 2\log\log q + 4)(q-1)}{(q^{n-1} - 1)} \\ &- \quad \frac{(4n^{5.2} + 2n\log\log q)}{q^{(n^2-14n+1)/4}\prod_{i=1}^{(n-1)/2}(q^{2i} - 1)}. \end{aligned}$$

If $n \geq 11$, or if $n \geq 9$ and $q \geq 7$, then $P_{G,G_0}(2) \geq 0.990$.

Theorem 5.1.16. *Let G be an almost simple group with socle $G_0 = \mathrm{P}\Omega_n^+(q)$ for $n \geq 8$.*

1. *If $G_0 = \mathrm{P}\Omega_n^+(2)$ for $n \geq 8$, then*

$$\begin{aligned} P_{G,G_0}(2) \geq 1 \quad &- \quad \frac{n + \log n + 8}{2^{(n-4)/2}(2^{n/2} - 1)} \\ &- \quad \frac{n^{5.2}}{2^{(n^2-14n-1)/4}(2^{n/2} - 1)\prod_{i=1}^{n/2-1}(2^{2i} - 1)}. \end{aligned}$$

2. If $G_0 = \mathrm{P}\Omega_n^+(3)$ for $n \geq 8$, then

$$P_{G,G_0}(2) \geq 1 - \frac{16n + 18\log n + 32}{3^{n/2}(3^{n/2}-1)} - \frac{8n^{5.2} + 4n\log\log 3}{3^{(n^2-14n)/4}(3^{n/2}-1)\prod_{i=1}^{n/2-1}(3^{2i}-1)}.$$

3. If $G_0 = \mathrm{P}\Omega_n^+(q)$ for $n \geq 8$ and $q \geq 4$, then

$$P_{G,G_0}(2) \geq 1 - \frac{(8n + 9\log n + 4\log\log q + 16)(q-1)}{(q^{n/2}-1)(q^{n/2-1}+1)} - \frac{8n^{5.2} + 4n\log\log q}{q^{(n^2-14n)/4}(q^{n/2}-1)\prod_{i=1}^{n/2-1}(q^{2i}-1)}.$$

If $n \geq 12$, or if $n \geq 10$ and $q \geq 4$, then $P_{G,G_0}(2) \geq 0.972$.

Theorem 5.1.17. *Let G be an almost simple group with socle $G_0 = \mathrm{P}\Omega_n^-(q)$ for $n \geq 8$, then*

$$P_{G,G_0}(2) \geq 1 - \frac{(3n + \log n + \log\log q + 16)(q-1)}{(q^{n/2}+1)(q^{n/2-1}-1)} - \frac{8n^{5.2} + 4n\log\log q}{q^{(n^2-14n)/4}(q^{n/2}+1)\prod_{i=1}^{n/2-1}(q^{2i}-1)}.$$

If $n \geq 12$, or if $n \geq 10$ and $q \geq 4$, then $P_{G,G_0}(2) \geq 0.968$.

We prove Theorems 5.1.12 – 5.1.17 together.

Proof of Theorems 5.1.12 – 5.1.17. Let G be an almost simple group with socle G_0 a classical group, and suppose G can be generated by 2 elements. Again, we let $\mathcal{M}$ be a set of conjugacy class representatives for maximal subgroups of G which do not contain G_0. By Theorem 5.1.9, $\mathcal{M}$ is the union of maximal subgroups lying in classes $\mathcal{C}_\mathcal{G}$, $\mathcal{E}$, and $\mathcal{S}'$. Let $m_\mathcal{G}(G)$, $m_\mathcal{E}(G)$, $m_{\mathcal{S}'}(G)$ denote the number of conjugacy classes of maximal subgroups of geometric type, the number of conjugacy classes of maximal subgroups lying in $\mathcal{E}$, and the number of conjugacy classes of maximal subgroups lying in $\mathcal{S}'$ respectively. Let $\rho(G_0)$ denote the minimal degree of a permutation representation of G_0. This is a lower bound for the index of maximal subgroups in G.

For maximal subgroups $M \in \mathcal{S}'$, we may obtain a better bound on the index of maximal subgroups in G by using Theorem 5.1.9. As $G_0 \leq G$ then

$$\frac{1}{[G:M]} \leq \frac{k}{|G_0|},$$

where $k = q^{6n}$ if $G_0 = \mathrm{PSU}_n(q)$, and $k = q^{3n}$ otherwise.

Combining the above we obtain an upper bound on the sum over maximal subgroups,

$$\begin{aligned}\sum_{M\in\mathcal{M}} \frac{1}{[G:M]} &\leq \sum_{M\in\mathcal{M}\cap\mathcal{C}_\mathcal{G}} \frac{1}{[G:M]} + \sum_{M\in\mathcal{M}\cap\mathcal{E}} \frac{1}{[G:M]} + \sum_{M\in\mathcal{M}\cap\mathcal{S}'} \frac{1}{[G:M]} \\ &\leq \frac{m_\mathcal{G}(G) + m_\mathcal{E}(G)}{\rho(G_0)} + \frac{m_{\mathcal{S}'}(G)k}{|G_0|} \\ &\leq \frac{m_\mathcal{G}(G) + m_\mathcal{E}(G)}{\rho(G_0)} + \frac{m(G)k}{|G_0|}.\end{aligned}$$

Lemmas 5.1.10 and 5.1.11 estimate $m_\mathcal{G}(G)$ and $m_\mathcal{E}(G)$, Theorem 5.1.1 bounds $m(G)$, Theorem 2.2.42 bounds $\rho(G_0)$, and the values for $|G_0|$ can be found in Chapter 2.

Then $P_{G,G_0}(2) \geq 1 - \sum_{M\in\mathcal{M}} 1/[G:M]$ bounds the probability. All these estimates are increasing with increasing n and q, so we may determine when these estimates show that the probability is greater than 0.927. □

5.2 Classical groups in dimension at most 12

Let $H = \mathrm{SL}_n(q)$, $\mathrm{Sp}_n(q)$, $\mathrm{SU}_n(q)$, $\Omega_n(q)$ or $\Omega_n^\pm(q)$, where $H/Z(H) = G_0$ is simple. For these groups there is maximal subgroup information in dimensions $n \leq 12$. Let $\mathcal{L}$ be a set of conjugacy class representatives for subgroups L of H where L is maximal, or where $L = M \cap H$ for M a novelty maximal subgroup of some extension K of H. In particular these K are such that $G_0 \leq K/Z(K) \leq \mathrm{Aut}(G_0)$.

If $G_0 \leq G \leq \mathrm{Aut}(G_0)$ where G can be generated by 2 elements, then by Lemmas 3.2.7 and 3.2.9 we may estimate the probability

$$P_{G,G_0}(2) \geq 1 - \sum_{L\in\mathcal{L}} \frac{1}{[H:L]}.$$

Tables in [10] list subgroups $L \in \mathcal{L}$ together with the number of conjugacy classes (in H) of each. When $G_0 = \mathrm{PSL}_2(q)$ we consider the sum more carefully, for all other possibilities for G_0 it suffices to find a fairly rough bound. We give the proof for $G_0 = \mathrm{PSL}_3(q)$ in more detail as an example, all the other estimates are calculated in a similar manner and much of the detail has been omitted. The method used to estimate $\sum_{L\in\mathcal{L}} 1/[H:L]$ is as follows. For $L \in \mathcal{L}$, we may determine the minimum index $[H : L]$ by checking all subgroups in the table, or we may estimate the index using the fact that $[H : L] = [G_0 : M]$ for some subgroup M of G_0. The latter is bounded below by $\rho(G_0)$, the minimum degree of a permutation representation of G. These values are given in Theorem 2.2.42. We may

restrict the values of q we consider as for some small values of q (usually $q = 2, 3$) there is a different formula for $\rho(G_0)$.

Then we count the number of conjugacy classes of subgroups L of H, that is, the number of subgroups in $\mathcal{L}$. There are often restrictions on q for each maximal subgroups, for example, some only occur for q odd, and others for q even. These restrictions can be used to reduce the bound on the number of subgroups in $\mathcal{L}$.

For subgroups L in class $\mathcal{C}_5$, that is stabilisers of subfields, we consider these subgroups together. In this case we get subgroups defined for some q_0, where $q_0^r = q$ for some prime r. If $q = p^f$ for some prime p, then the number of possibilities for q_0 is equal to the number of possibilities for r, which is the number of prime divisors of f. This in turn is bounded by $\log \log q$. The order of such subgroups are bounded using the fact that $q_0 \leq q^{1/2}$. We usually consider the contribution to the sum $\sum_{L \in \mathcal{L}} 1/[H : L]$ of subgroups in $\mathcal{C}_5$ together and show $\sum_{L \cap \mathcal{C}_5} 1/[H : L] \leq 1/\rho(G_0)$.

In each case we obtain an estimate for $P_{G,G_0}(2)$ which is increasing with increasing q. The probability estimates are not always good enough for some cases where n and q are both small. In these cases probability estimates have been calculated in GAP [28] and MAGMA [8], or from tables of maximal subgroups in the ATLAS [17]. Computational estimates are given in Section 5.3.

5.2.1 Almost simple groups with socle $\mathrm{PSL}_n(q)$

First we calculate the probability for groups with socle $G_0 = \mathrm{PSL}_2(q)$. We consider $q \geq 4$, as otherwise G_0 is not simple.

Lemma 5.2.1. *Let $G_0 = \mathrm{PSL}_2(q)$ for $q \geq 4$, and let $G_0 \leq G \leq \mathrm{Aut}(G_0)$. Then*

$$P_{G,G_0}(2) \geq 1 - \frac{3q^2 + 3q + 286}{q(q^2 - 1)}.$$

If $q \geq 47$ then $P_{G,G_0}(2) \geq 0.932$.

Proof. Let $H = \mathrm{SL}_2(q)$. Let $\mathcal{L}$ be a set of conjugacy class representatives for maximal subgroups of H, and subgroups of H which are intersections with H of novelty maximal subgroups of some extension of H. These subgroups L are given in [10], and the appropriate table is reproduced as Table 5.2. Here c denotes the number of conjugacy classes in H, and the N on some rows denotes that these are intersections of H with novelty maximal subgroups of some extension of H.

By Lemma 3.2.9,

$$P_{G,G_0}(2) \geq 1 - \sum_{L \in \mathcal{L}} \frac{1}{[H : L]}.$$

Class	Subgroup	Notes	c
$\mathcal{C}_1$	$[q]:(q-1)$		1
$\mathcal{C}_2$	$Q_{2(q-1)}$	$q \neq 5,7,8,11; q$ odd	1
		N if $q = 7, 11$	1
		N if $q = 9$	1
$\mathcal{C}_2$	$D_{2(q-1)}$	q even	1
$\mathcal{C}_3$	$Q_{2(q+1)}$	$q \neq 7, 9; q$ odd	1
		N if $q = 7$	1
		N if $q = 9$	1
$\mathcal{C}_3$	$D_{2(q+1)}$	q even	1
$\mathcal{C}_5$	$\mathrm{SL}_2(q_0).2$	$q = q_0^r$, q odd, $r = 2$	2
$\mathcal{C}_5$	$\mathrm{SL}_2(q_0)$	$q = q_0^r$, q odd, r odd prime	1
$\mathcal{C}_5$	$\mathrm{PSL}_2(q_0)$	$q = q_0^r$, q even, $q_0 \neq 2$, r prime	1
$\mathcal{C}_6$	$2_-^{1+2}.S_3$	$q = p \equiv \pm 1 \mod 8$	2
$\mathcal{C}_6$	$2_-^{1+2}:3$	$q = p \equiv \pm 3, 5, \pm 13 \mod 40$	1
		N if $q = p \equiv \pm 11, \pm 19 \mod 40$	1
$\mathcal{S}$	$2^{\cdot} A_5$	$q = p \equiv \pm 1 \mod 10$	2
		$q = p^2$, $p \equiv \pm 3 \mod 10$	2

Table 5.2: Maximal subgroups of $\mathrm{SL}_2(q)$

The order of $\mathrm{SL}_2(q)$ is $q(q^2-1)$ and we calculate $\sum_{L\in\mathcal{L}} |L|$.

First suppose $q = p$, for some odd prime $p \geq 5$. We get at most one conjugacy class of subgroups of each of the following types: $[q]:(q-1)$, $Q_{2(q-1)}$ and $Q_{2(q+1)}$. We do not get any subgroups in $\mathcal{C}_5$. Depending on the value of p we may have 2 conjugacy classes of subgroups of the form $2_-^{1+2}.S_3$, or one class of the form $2_-^{1+2}:3$. Note that we cannot have both of these types at once. Finally, we have at most two conjugacy classes of subgroups in $\mathcal{S}$, and these subgroups have order 120. Then,

$$\begin{aligned}\sum_{L\in\mathcal{L}} |L| &= q(q-1) + 2(q-1) + 2(q+1) + 2\times 48 + 2\times 120 \\ &= q^2 + 3q + 336 \\ &\leq 3q^2 + 3q + 286.\end{aligned}$$

Next suppose $q = p^2$ for odd p. Then $q \geq 9$. In this case we get at most one conjugacy class of each of the following subgroups: $[q]:(q-1)$, $Q_{2(q-1)}$, $Q_{2(q+1)}$. We get 2 conjugacy classes of subgroups in $\mathcal{L}$ of the form $\mathrm{SL}_2(p).2$.

Finally we have at most 2 subgroups of the form $2^{\cdot}A_5$. Then

$$\begin{aligned}\sum_{L\in\mathcal{L}}|L| &= q(q-1)+2(q-1)+2(q+1)+2\times 2p(p^2-1)+2\times 120\\ &= q^2+3q+4q^{1/2}(q-1)+240\\ &= q^2+4q^{3/2}+3q-4q^{1/2}+240\\ &\leq 3q^2+3q+286.\end{aligned}$$

Next let $q=p^f$, where p is odd, and $f\geq 3$. Then we get one conjugacy class in $\mathcal{L}$ of each of the subgroups $[q]:(q-1)$, $Q_{2(q-1)}$ and $Q_{2(q+1)}$. If $q=q_0^2$ for some q_0, then there are two conjugacy classes of subgroups of the form $\mathrm{SL}_2(q_0).2$. These subgroups have order $2q^{1/2}(q-1)$. If $q=q_0^r$ for some q_0, and some odd prime r, then we get one conjugacy class of subgroups of the form $\mathrm{SL}_2(q_0)$. So there is one conjugacy class of subgroups of this form for each possibility for r. The number of possibilities for r is bounded by the number of distinct prime divisors of f, and this is bounded above by $\log\log q$. As $r\geq 3$, then $|\mathrm{SL}_2(q_0)|=q_0(q_0^2-1)\leq q^{1/3}(q^{2/3}-1)$. So,

$$\begin{aligned}\sum_{L\in\mathcal{L}}|L| &\leq q(q-1)+2(q-1)+2(q+1)\\ &+ 2\times 2q^{1/2}(q-1)+(\log\log q)q^{1/3}(q^{2/3}-1)\\ &\leq 2q^2+3q+4q^{3/2}-4q^{1/2}\\ &\leq 3q^2+3q+286.\end{aligned}$$

Finally suppose $q=2^f$ for $f\geq 2$. We get one conjugacy class of subgroups in $\mathcal{L}$ of the following $[q]:(q-1)$, $D_{2(q-1)}$, $D_{2(q+1)}$. We get one class of subgroups of the form $\mathrm{PSL}_2(q_0)$ for each r such that $q=q_0^r$, $q_0\neq 2$ and r prime. The number of possibilities for r is bounded by $\log\log q$, and $|\mathrm{PSL}_2(q_0)|\leq q^{1/2}(q-1)$. There are no other subgroups in $\mathcal{L}$ as they occur only for odd values of q.

$$\begin{aligned}\sum_{L\in\mathcal{L}}|L| &\leq q(q-1)+2(q-1)+2(q+1)+(\log\log q)q^{1/2}(q-1)\\ &\leq 2q^2+2q\\ &\leq 3q^2+3q+286.\end{aligned}$$

Then for all values of q,

$$P_{G,G_0}(2)\geq 1-\frac{3q^2+3q+286}{q(q^2-1)}.$$

This estimate is increasing with increasing q, and we establish that if $q\geq 47$ then $P_{G,G_0}(2)\geq 0.932$. □

Class	Subgroup	Notes	c
$\mathcal{C}_1$	$[q^2] : \mathrm{GL}_2(q)$		2
$\mathcal{C}_1$	$[q^{1+2}] : (q-1)^2$	N	1
$\mathcal{C}_1$	$\mathrm{GL}_2(q)$	N	1
$\mathcal{C}_2$	$(q-1)^2 : S_3$	$q \geq 5$	1
$\mathcal{C}_3$	$(q^2+q+1) : 3$	$q \neq 4$	1
		N if $q = 4$	1
$\mathcal{C}_5$	$\mathrm{SL}_3(q_0).(\frac{q-1}{q_0-1}, 3)$	$q = q_0^r$, r prime	$(\frac{q-1}{q_0-1}, 3)$
$\mathcal{C}_6$	$3_+^{1+2} : Q_8.\frac{(q-1,9)}{3}$	$p = q \equiv 1 \mod 3$	$(q-1,9)/3$
$\mathcal{C}_8$	$(q-1,3) \times \mathrm{SO}_3(q)$	q odd	$(q-1,3)$
$\mathcal{C}_8$	$(q_0-1,3) \times \mathrm{SU}_3(q)$	$q = q_0^2$	$(q_0-1,3)$
$\mathcal{S}$	$(q-1,3) \times \mathrm{PSL}_2(7)$	$q = p \equiv 1,2,4 \mod 7$, $p \neq 2$	$(q-1,3)$
$\mathcal{S}$	$3^{\cdot} A_6$	$q = p \equiv 1,4 \mod 15$	3
		$q = p^2$, $p \equiv 2,3 \mod 5$, $p \neq 3$	3

Table 5.3: Maximal subgroups of $\mathrm{SL}_3(q)$

Lemma 5.2.2. *Let $G_0 = \mathrm{PSL}_3(q)$ and let $G_0 \leq G \leq \mathrm{Aut}(G_0)$. Then*

$$P_{G,G_0}(2) \geq 1 - \frac{18}{q^2+q+1},$$

and if $q \geq 17$ then $P_{G,G_0}(2) \geq 0.941$.

Proof. Let $H = \mathrm{SL}_3(q)$, and let $\mathcal{L}$ be a set of conjugacy class representatives for subgroups L of H where L is maximal, or where $L = M \cap H$ for M a novelty maximal subgroup of some extension of H. By Lemmas 3.2.7 and 3.2.9,

$$P_{G,G_0}(2) \geq 1 - \sum_{L \in \mathcal{L}} \frac{1}{[H:L]}.$$

Subgroups in $\mathcal{L}$ are listed in [10] and reproduced as Table 5.3. We use this list to estimate $\sum_{L \in \mathcal{L}} 1/[H:L]$. The minimal index of a subgroup L of H is q^2+q+1 which corresponds to $\rho(G_0)$ (given in Theorem 2.2.42).

There are 2 conjugacy classes of subgroups of the form $L = [q^2] : \mathrm{GL}_2(q)$. Next we have at most one conjugacy class of subgroups in $\mathcal{L}$ of each of the following: $[q^{1+2}] : (q-1)$, $\mathrm{GL}_2(q)$, $(q-1)^2 : S_3$ and $(q^2+q+1) : 3$. Each of these subgroups contributes at most $1/(q^2+q+1)$ to the sum $\sum_{L \in \mathcal{L}} 1/[H:L]$.

If $q = q_0^r$ for some prime r, then there are at most 3 subgroups in $\mathcal{L} \cap \mathcal{C}_5$ of the form $\mathrm{SL}_3(q_0).(\frac{q-1}{q_0-1}, 3)$ for every possible q_0. So if $q = p^f$ for some prime p, the number of possibilities for q_0 is the number of possibilities for r which is the number of prime divisors of f. This is bounded above by $\log \log q$. As $q_0 \leq q^{1/2}$, the order of $\mathrm{SL}_3(q_0).(\frac{q-1}{q_0-1}, 3)$ is at most $3q^{3/2}(q-1)(q^{3/2}-1)$.

Then,

$$\sum_{L\in\mathcal{L}\cap\mathcal{C}_5}\frac{1}{[H:L]}\leq\frac{3(\log\log q)(3q^{3/2}(q-1)(q^{3/2}-1))}{q^3(q^2-1)(q^3-1)}\leq\frac{1}{q^2+q+1}.$$

If $p=q\equiv 1 \mod 3$, then there are at most 3 conjugacy classes of subgroups of the form $3_+^{1+2}:Q_8.\frac{(q-1,9)}{3}$. If q is odd then there are at most $(3,q-1)$ subgroups in $\mathcal{L}$ of the form $(q-1,3)\times \mathrm{SO}_3(q)$. If $q=q_0^2$, then there are $(q_0-1,3)$ subgroups in $\mathcal{L}$ of the form $(q_0-1,3)\times \mathrm{SU}_3(q_0)$.

Finally we consider subgroups in $\mathcal{L}\cap\mathcal{S}$. If $q=p\equiv 1,2,4 \mod 7$, there are at most 3 subgroups in $\mathcal{L}$ of the form $(3,q-1)\times \mathrm{PSL}_2(7)$. There are at most 3 conjugacy classes of subgroups of the form $3^{\cdot}A_6$.

Summarising, if $q=p^f$ for some prime p and some $f\geq 2$, then we get subgroups in $\mathcal{C}_5$ which contribute at most $1/(q^2+q+1)$ to the sum $\sum_{L\in\mathcal{L}}1/[H:L]$. There are at most 15 other subgroups in $\mathcal{L}$, each of which has index at least (q^2+q+1). Otherwise $q=p$ for some prime p. Then there no subgroups in $\mathcal{L}\cap\mathcal{C}_5$, and there are at most 18 subgroups in $\mathcal{L}$.

Then, for all values of q,

$$\sum_{L\in\mathcal{L}}\frac{1}{[H:L]}\leq\frac{18}{q^2+q+1}$$

and so

$$P_{G,G_0}(2)\geq 1-\frac{18}{q^2+q+1}.$$

This estimate is increasing with increasing q. □

Lemma 5.2.3. *Let $G_0=\mathrm{PSL}_4(q)$ for $q\geq 3$, and let $G_0\leq G\leq \mathrm{Aut}(G_0)$, where G can be generated by 2 elements. Then*

$$P_{G,G_0}(2)\geq 1-\frac{30}{q^3+q^2+q+1},$$

and if $q\geq 8$ then $P_{G,G_0}(2)\geq 0.948$.

Proof. Let $H=\mathrm{SL}_4(q)$, and let $\mathcal{L}$ be a set of conjugacy class representatives for subgroups L of H where L is maximal, or where $L=M\cap H$ for M a novelty maximal subgroup of some extension of H. By Lemmas 3.2.7 and 3.2.9,

$$P_{G,G_0}(2)\geq 1-\sum_{L\in\mathcal{L}}\frac{1}{[H:L]}.$$

Subgroups in $\mathcal{L}$ are listed in [10] and we estimate $\sum_{L\in\mathcal{L}}1/[H:L]$. The minimal index of a subgroup L of H is $\rho(G_0)=(q^4-1)/(q-1)=q^3+q^2+q+1$ (see Theorem 2.2.42).

First suppose $q=p^f$ for some prime p and some $f\geq 2$. We get subgroups in $\mathcal{L}\cap\mathcal{C}_5$ of the form $\mathrm{SL}_4(q_0).[(\frac{q-1}{q_0-1},4)]$ for each possibility for q_0, where

$q = q_0^r$, and r is prime. Then the number of possibilities for q_0 is bounded above by $\log\log q$. We bound the order of these subgroups using the fact that $q_0 \leq q^{1/2}$. For each q_0, there are $(\frac{q-1}{q_0-1}, 4)$ conjugacy classes of such maximal sugbroups. Then

$$\sum_{L\in\mathcal{L}\cap\mathcal{C}_5} \frac{1}{[H:L]} \leq \frac{4q^3 \log\log q(q-1)(q^{3/2}-1)(q^2-1)}{|H|} \leq \frac{1}{(q^3+q^2+q+1)}.$$

If $q = p^f$ for $f \geq 2$, then there are at most 22 other conjugacy classes of subgroups L as described above. If $q = p$, then there are at most 30 subgroups in $\mathcal{L}$.

Then, for all q,

$$P_{G,G_0}(2) \geq 1 - \sum_{L\in\mathcal{L}} \frac{1}{[H:L]} \geq 1 - \frac{30}{q^3+q^2+q+1}.$$

This estimate is increasing with increasing q and so we obtain the lower bound for $q \geq 8$. □

5.2.2 Almost simple groups with socle $\mathrm{PSp}_n(q)$

As $\mathrm{PSp}_2(q) \cong \mathrm{PSL}_2(q)$ and n is even, we only consider $n \geq 4$. We exclude $\mathrm{PSp}_4(2)$ as it is not simple.

Lemma 5.2.4. *Let $G_0 = \mathrm{PSp}_4(q)$ for $q \geq 3$, and let $G_0 \leq G \leq \mathrm{Aut}(G_0)$. Then*

$$P_{G,G_0}(2) \geq 1 - \frac{12}{q^3+q^2+q+1},$$

and if $q \geq 7$ then $P_{G,G_0}(2) \geq 0.970$.

Proof. Let $H = \mathrm{Sp}_4(q)$ for $q \geq 3$, and let $\mathcal{L}$ be a set of conjugacy class representatives for subgroups L of H where L is maximal, or where $L = M \cap H$ for M a novelty maximal subgroup of some extension of H. By Lemmas 3.2.7 and 3.2.9,

$$P_{G,G_0}(2) \geq 1 - \sum_{L\in\mathcal{L}} \frac{1}{[H:L]}.$$

Subgroups in $\mathcal{L}$ are listed in [10]. There are separate tables of maximal subgroups for q odd and q even as when q is even $\mathrm{Aut}(\mathrm{PSp}_4(q))$ has a graph automorphism. We use these tables to estimate the sum $\sum_{L\in\mathcal{L}} 1/[H:L]$. The minimal index of a subgroup L of H is $(q^4-1)/(q-1) = q^3+q^2+q+1$ which follows from Theorem 2.2.42.

First consider subgroups in $\mathcal{C}_5$. Recall $q = p^f$ for some prime p. We get subgroups in $\mathcal{L}\cap\mathcal{C}_5$ of the form $\mathrm{Sp}_4(q_0).[(\frac{q-1}{q_0-1}, 4)]$ for each q_0 such that $q = q_0^r$, for some prime r. The number of possibilities for q_0 is given by the

number of prime divisors of f, which is bounded above by $\log\log q$. For each q_0, there are $(2, r)$ classes of these subgroups in $\mathcal{L} \cap \mathcal{C}_5$. Then

$$\sum_{L \in \mathcal{L} \cap \mathcal{C}_5} \frac{1}{[H : L]} \leq \frac{1}{q^3 + q^2 + q + 1}.$$

There are at most 11 other subgroups in $\mathcal{L}$.

Then, for all q,

$$P_{G,G_0}(2) \geq 1 - \frac{12}{q^3 + q^2 + q + 1}.$$

□

Lemma 5.2.5. *Let $G_0 = \mathrm{PSp}_6(q)$ for $q \geq 3$, and let $G_0 \leq G \leq \mathrm{Aut}(G_0)$. Then*

$$P_{G,G_0}(2) \geq 1 - \frac{22}{q^5 + q^4 + q^3 + q^2 + q + 1}$$

and $P_{G,G_0}(2) \geq 0.939$.

Proof. Let $H = \mathrm{Sp}_6(q)$, and let $\mathcal{L}$ be a set of conjugacy class representatives for subgroups L of H where L is maximal, or where $L = M \cap H$ for M a novelty maximal subgroup of some extension of H. By Lemmas 3.2.7 and 3.2.9,

$$P_{G,G_0}(2) \geq 1 - \sum_{L \in \mathcal{L}} \frac{1}{[H : L]}.$$

Subgroups in $\mathcal{L}$ are listed in [10] and we use this to estimate $\sum_{L \in \mathcal{L}} 1/[H : L]$. The minimal index of a subgroup L of H is $(q^6-1)/(q-1) = q^5+q^4+q^3+q^2+q+1$ corresponding to the minimal degree of a permutation representation of G_0 from Theorem 2.2.42.

First suppose $q = p^f$, for some prime p and some $f \geq 2$. Then we get subgroups in $\mathcal{L} \cap \mathcal{C}_5$ whenever $q = q_0^r$ for some q_0 and some prime r. It can be shown that

$$\sum_{L \in \mathcal{L} \cap \mathcal{C}_5} \frac{1}{[H : L]} \leq \frac{1}{q^5 + q^4 + q^3 + q^2 + q + 1}.$$

There are at most 14 other subgroups in $\mathcal{L}$. If $q = p$ then there are at most 22 subgroups in $\mathcal{L}$.

Then, for any $q \geq 3$,

$$P_{G,G_0}(2) \geq 1 - \frac{22}{q^5 + q^4 + q^3 + q^2 + q + 1}$$

and this estimate is increasing with increasing q. □

Lemma 5.2.6. *Let $G_0 = \mathrm{PSp}_8(q)$ and let $G_0 \leq G \leq \mathrm{Aut}(G_0)$. Then*

$$P_{G,G_0}(2) \geq 1 - \frac{22}{q^7+q^6+q^5+q^4+q^3+q^2+q+1}$$

and if $q \geq 3$, then $P_{G,G_0}(2) \geq 0.993$.

Proof. Let $H = \mathrm{Sp}_8(q)$, and let $\mathcal{L}$ be a set of conjugacy class representatives for subgroups L of H where L is maximal, or where $L = M \cap H$ for M a novelty maximal subgroup of some extension of H. By Lemmas 3.2.7 and 3.2.9,

$$P_{G,G_0}(2) \geq 1 - \sum_{L \in \mathcal{L}} \frac{1}{[H:L]}.$$

Subgroups in $\mathcal{L}$ are listed in [10] and we use this to estimate $\sum_{L\in\mathcal{L}} 1/[H:L]$. The index of a subgroup L of H is bounded below by $q^7+q^6+q^5+q^4+q^3+q^2+q+1$ which follows from Theorem 2.2.42.

If $q = p^f$ for some prime p, and some $f \geq 2$, then we get subgroups of the form $\mathrm{Sp}_8(q_0).(d,r)$ lying in $\mathcal{L} \cap \mathcal{C}_5$. We get at most 2 conjugacy classes of these subgroups for each q_0, $q_0 \leq q^{1/2}$, and the number of possibilities for q_0 is at most $\log\log q$. Then

$$\sum_{L \in \mathcal{L}\cap\mathcal{C}_5} \frac{1}{[H:L]} \leq \frac{1}{q^7+q^6+q^5+q^4+q^3+q^2+q+1}.$$

There are at most 19 other subgroups in $\mathcal{L}$ if $f \geq 2$.

Next suppose $q = p$ for some prime p. In this case we do not get subgroups in $\mathcal{C}_5$ and there are at most 22 subgroups in $\mathcal{L}$.

Then, for all q,

$$\sum_{L \in \mathcal{L}} \frac{1}{[H:L]} \leq \frac{22}{q^7+q^6+q^5+q^4+q^3+q^2+q+1}$$

and so

$$P_{G,G_0}(2) \geq 1 - \frac{22}{q^7+q^6+q^5+q^4+q^3+q^2+q+1},$$

and this estimate is increasing with increasing q. □

5.2.3 Almost simple groups with socle $\mathrm{PSU}_n(q)$

Recall $\mathrm{PSU}_2(q) \cong \mathrm{PSL}_2(q)$. So we only consider unitary groups in dimensions $n \geq 3$. We also exclude $G = \mathrm{PSU}_3(2)$, as it is not simple.

For $\mathrm{PSU}_3(q)$ we only consider $q \geq 7$ as the minimal index of a maximal subgroup is smaller for $q = 5$, and for $q \leq 5$, the rough bound is not good enough for us anyway. For $q \leq 5$ it will be easy to calculate probability estimates computationally.

Lemma 5.2.7. *Let $G_0 = \mathrm{PSU}_3(q)$ for $q \geq 7$, and let $G_0 \leq G \leq \mathrm{Aut}(G_0)$. Then*

$$P_{G,G_0}(2) \geq 1 - \frac{16}{q^3+1}$$

and $P_{G,G_0}(2) \geq 0.953$.

Proof. Let $H = \mathrm{SU}_3(q)$, and let $\mathcal{L}$ be a set of conjugacy class representatives for subgroups L of H where L is maximal, or where $L = M \cap H$ for M a novelty maximal subgroup of some extension of H. By Lemmas 3.2.7 and 3.2.9,

$$P_{G,G_0}(2) \geq 1 - \sum_{L \in \mathcal{L}} \frac{1}{[H:L]}.$$

Subgroups in $\mathcal{L}$ are listed in [10] and we use this to estimate $\sum_{L\in\mathcal{L}} 1/[H:L]$. The minimal index of a subgroup L of H is q^3+1 which corresponds to subgroups of the form $L = [q^{1+2}] : (q^2-1)$.

If $q = p^f$ for some $f \geq 2$, then we get subgroups in $\mathcal{L} \cap \mathcal{C}_5$ of the form $\mathrm{SU}_3(q_0).(\frac{q+1}{q_0+1}, 3)$ for $q = q_0^r$ for odd primes r. The number of possibilities for q_0 is bounded by the number of prime divisors of f, which is less than $\log\log q$. Then

$$\sum_{L \in \mathcal{L}\cap\mathcal{C}_5} \frac{1}{[H:L]} \leq \frac{1}{q^3+1}.$$

There are at most 7 other subgroups in $\mathcal{L}$, each of which contributes at most $1/(q^3+1)$ to the sum $\sum_{L\in\mathcal{L}} 1/[H:L]$. If $q = p$, then there are at most 16 subgroups in $\mathcal{L}$.

Then, for all q,

$$\sum_{L \in \mathcal{L}} \frac{1}{[H:L]} \leq \frac{16}{q^3+1}$$

and so

$$P_{G,G_0}(2) \geq 1 - \frac{16}{q^3+1}.$$

□

Lemma 5.2.8. *Let $G_0 = \mathrm{PSU}_4(q)$ for $q \geq 3$ and let $G_0 \leq G \leq \mathrm{Aut}(G_0)$. Then*

$$P_{G,G_0}(2) \geq 1 - \frac{28}{q^4+q^3+q+1},$$

and if $q \geq 5$ then $P_{G,G_0}(2) \geq 0.962$.

Proof. Let $H = \mathrm{SU}_4(q)$, and let $\mathcal{L}$ be a set of conjugacy class representatives for subgroups L of H where L is maximal, or where $L = M \cap H$ for M a novelty maximal subgroup of some extension of H. By Lemmas 3.2.7 and 3.2.9,

$$P_{G,G_0}(2) \geq 1 - \sum_{L \in \mathcal{L}} \frac{1}{[H:L]}.$$

Subgroups in $\mathcal{L}$ are listed in [10] and we use this to estimate $\sum_{L\in\mathcal{L}} 1/[H:L]$. The minimal index of a subgroup L of H is q^4+q^3+q+1 which comes from Theorem 2.2.42.

If $q = p$, for some prime p, there are at most 28 conjugacy classes of subgroups L of H where L is maximal, or where $L = M \cap H$, for M a novelty maximal subgroup of some extension of H.

If $q = p^f$ for some $f \geq 2$, we get subgroups in $\mathcal{L}\cap\mathcal{C}_5$ of the form $\mathrm{SU}_4(q_0)$ for $q = q_0^f$ and we may bound

$$\sum_{L\in\mathcal{L}\cap\mathcal{C}_5} \frac{1}{[H:L]} \leq \frac{1}{q^4+q^3+q+1}.$$

There are at most 16 other subgroups in $\mathcal{L}$.

Then, for all q,

$$P_{G,G_0}(2) \geq 1 - \frac{28}{q^4+q^3+q+1}.$$

□

Lemma 5.2.9. *Let $G_0 = \mathrm{PSU}_5(q)$ and let $G_0 \leq G \leq \mathrm{Aut}(G_0)$. Then*

$$P_{G,G_0}(2) \geq 1 - \frac{26}{(q^5+1)(q^2+1)}$$

and if $q \geq 3$ then $P_{G,G_0}(2) \geq 0.989$.

Proof. Let $H = \mathrm{SU}_5(q)$, and let $\mathcal{L}$ be a set of conjugacy class representatives for subgroups L of H where L is maximal, or where $L = M \cap H$ for M a novelty maximal subgroup of some extension of H. By Lemmas 3.2.7 and 3.2.9,

$$P_{G,G_0}(2) \geq 1 - \sum_{L\in\mathcal{L}} \frac{1}{[H:L]}.$$

Subgroups in $\mathcal{L}$ are listed in [10] and we use this to estimate $\sum_{L\in\mathcal{L}} 1/[H:L]$. The minimal index of a subgroup L of H is $(q^2+1)(q^5+1)$ which corresponds to subgroups of the form $L = [q^{1+6}] : \mathrm{SU}_3(q).(q^2-1)$.

If $q = p^f$ for some prime p, and some $f \geq 2$, then we get subgroups in $\mathcal{C}_5$ of the form $\mathrm{SU}_5(q_0).(\frac{q+1}{q_0+1}, 5)$, for $q = q_0^r$ for some odd prime r. Then we can show

$$\sum_{L\in\mathcal{L}\cap\mathcal{C}_5} \frac{1}{[H:L]} \leq \frac{1}{(q^2+1)(q^5+1)}.$$

There are at most 16 other subgroups in $\mathcal{L}$, each of which contributes at most $1/(q^2+1)(q^5+1)$ to the sum $\sum_{L\in\mathcal{L}} 1/[H:L]$. Now suppose $q = p$ for some prime p. For any given prime p, there are at most 26 subgroups in $\mathcal{L}$.

Then,

$$\sum_{L\in\mathcal{L}} \frac{1}{[H:L]} \leq \frac{26}{(q^2+1)(q^5+1)},$$

and so we obtain the following estimate

$$P_{G,G_0}(2) \geq 1 - \frac{26}{(q^2+1)(q^5+1)}.$$

□

Lemma 5.2.10. *Let $G_0 = \mathrm{PSU}_6(q)$ for $q \geq 3$ and let $G_0 \leq G \leq \mathrm{Aut}(G_0)$. Then*

$$P_{G,G_0}(2) \geq 1 - \frac{67}{(q^5+1)(q^4+q^2+1)}$$

and $P_{G,G_0}(2) \geq 0.996$.

Proof. Let $H = \mathrm{PSU}_6(q)$, and let $\mathcal{L}$ be a set of conjugacy class representatives for subgroups L of H where L is maximal, or where $L = M \cap H$ for M a novelty maximal subgroup of some extension of H. By Lemmas 3.2.7 and 3.2.9,

$$P_{G,G_0}(2) \geq 1 - \sum_{L\in\mathcal{L}} \frac{1}{[H:L]}.$$

Subgroups in $\mathcal{L}$ are listed in [10] and we use this to estimate $\sum_{L\in\mathcal{L}} 1/[H:L]$. The minimal index of a subgroup L of H is $(q^5+1)(q^4+q^2+1)$ which corresponds to subgroups of the form $L = [q^{1+8}] : \mathrm{SU}_4(q).(q-1)$.

When $q = p^f$ for $f \geq 2$, subgroups in $\mathcal{L} \cap \mathcal{C}_5$ contribute at most $1/(q^5+1)(q^4+q^2+1)$ to the sum $\sum_{L\in\mathcal{L}} 1/[H:L]$. There are at most 22 other subgroups in $\mathcal{L}$. Now suppose $q = p$. Then there are at most 67 subgroups in $\mathcal{L}$.

Then, for all q,

$$\sum_{L\in\mathcal{L}} \frac{1}{[H:L]} \leq \frac{67}{(q^5+1)(q^4+q^2+1)},$$

and so

$$P_{G,G_0}(2) \geq 1 - \frac{67}{(q^5+1)(q^4+q^2+1)}.$$

This is increasing with increasing q, and so $P_{G,G_0}(2) \geq 0.996$. □

5.2.4 Almost simple groups with socle $\mathrm{P}\Omega^{\epsilon}_n(q)$

Recall that if n is odd, we assume that q is odd and $\mathrm{P}\Omega_n(q) = \Omega_n(q)$ is simple.

Lemma 5.2.11. *Let $G_0 = \Omega_7(q)$, and let $G_0 \leq G \leq \mathrm{Aut}(G_0)$. Then*

$$P_{G,G_0}(2) \geq 1 - \frac{15}{q^3(q^2+q+1)},$$

and $P_{G,G_0}(2) \geq 0.957$.

Proof. Let $\mathcal{M}$ be a set of conjugacy class representatives for maximal subgroups M of G_0, or intersections with G_0 of novelty maximal subgroups of some extension of G_0. By Lemma 3.2.7,

$$P_{G,G_0}(2) \geq 1 - \sum_{M \in \mathcal{M}} \frac{1}{[G_0 : M]}.$$

The subgroups in $\mathcal{M}$ are listed in [10]. By Theorem 2.2.42, $[G_0 : M] \geq q^3(q^2+1+1)$.

If $q = p^f$ for some prime p and some $f \geq 2$, then we get subgroups of the forms $\Omega_7(q_0)$ where $q = q_0^r$ for some odd prime r, and $\mathrm{SO}_7(q_0)$ for $r = 2$. In both these cases we may bound the order of such subgroups by noting that $q_0 \leq q^{1/3}$ and $q_0 \leq q^{1/2}$ respectively, and in each case the number of such subgroups is bounded by the number of possibilities for r which is at most $\log\log q$. Each of these families of groups contributes at most $1/(q^3(q^2+q+1))$ to the sum $\sum_{L \in \mathcal{L}} 1/[G_0 : L]$. There are at most 13 other subgroups in $\mathcal{L}$. Otherwise $q = p$, and there are at most 15 subgroups in $\mathcal{L}$.

Then, for all q,

$$\sum_{L \in \mathcal{L}} \frac{1}{[G_0 : L]} \leq \frac{15}{q^3(q^2+q+1)},$$

and so

$$P_{G,G_0}(2) \geq 1 - \frac{15}{q^3(q^2+q+1)}.$$

This is increasing with increasing q, and as $q \geq 3$, we obtain $P_{G,G_0}(2) \geq 0.957$. □

Lemma 5.2.12. *Let $G_0 = \mathrm{P}\Omega_8^+(q)$ for $q \geq 2$ and let $G_0 \leq G \leq \mathrm{Aut}(G_0)$ where G can be generated by two elements. Then*

$$P_{G,G_0}(2) \geq 1 - \frac{76}{q^3(q^3+q^2+q+1)}$$

and if $q \geq 3$ then $P_{G,G_0}(2) \geq 0.929$.

Proof. Let $H = \Omega_8^+(q)$. Let $\mathcal{L}$ be a set of conjugacy class representatives for subgroups L of H where L is maximal, or $L = M \cap H$, for M a novelty

maximal subgroup of some extension of H. By Lemmas 3.2.7 and 3.2.9 we estimate

$$P_{G,G_0}(2) \geq 1 - \sum_{L \in \mathcal{L}} \frac{1}{[H:L]}.$$

The possibilities for $\mathcal{L}$ are given in [10]. From this list we see that the minimal index for a subgroup is at least $1/q^3(q^3+q^2+q+1)$.

If $q = p$, then there are at most 69 subgroups in $\mathcal{L}$. Otherwise $q = p^f$ for some $f \geq 2$. In this case we get at most one conjugacy class of subgroups of the form $\Omega_8^+(q_0)$ for each prime divisor r of f (as $q_0^r = p^f$). In this case $q_0 \leq q^{1/2}$. Then

$$\sum_{\substack{L \in \mathcal{L} \\ L \cong \Omega_8^+(q_0), q_0^r = q \\ r \text{ prime}}} \frac{1}{[H:L]} \leq \frac{(\log q)|\Omega_8^+(q_0)|}{|\Omega_8^+(q)|} \leq \frac{1}{q^3(q^3+q^2+q+1)}.$$

There are at most 75 other conjugacy classes of subgroups in $\mathcal{L}$ and so for any q,

$$\sum_{L \in \mathcal{L}} \frac{1}{[H:L]} \leq \frac{76}{q^3(q^3+q^2+q+1)}.$$

□

Lemma 5.2.13. *Let $G_0 = \mathrm{P}\Omega_8^-(q)$, and let $G_0 \leq G \leq \mathrm{Aut}(G_0)$. Then*

$$P_{G,G_0}(2) \geq 1 - \frac{14}{(q^2+q+1)(q^4+1)}$$

and if $q \geq 3$ then $P_{G,G_0}(2) \geq 0.986$.

Proof. Let $H = \Omega_8^-(q)$, and let $\mathcal{L}$ be a set of conjugacy class representatives for subgroups L of H where L is maximal, or where $L = M \cap H$ for M a novelty maximal subgroup of some extension of H. By Lemmas 3.2.7 and 3.2.9,

$$P_{G,G_0}(2) \geq 1 - \sum_{L \in \mathcal{L}} \frac{1}{[H:L]}.$$

Subgroups in $\mathcal{L}$ are listed in [10] and we use this to estimate $\sum_{L \in \mathcal{L}} 1/[H:L]$. The minimal index of a subgroup L of H is $(q^2+q+1)(q^4+1)$ which corresponds to subgroups of the form $L = [q^6] : (\frac{q-1}{(q-1,2)} \times \Omega_6^-(q)).(q-1,2)$.

Let $q = p^f$ for some prime p and $f \geq 2$. We get one subgroup of the form $\Omega_8^-(q_0)$ in $\mathcal{L}$ for each q_0 such that $q = q_0^r$ for r an odd prime. Then there are at most $r \leq \log\log q$ subgroups in $\mathcal{L} \cap \mathcal{C}_5$. As $q_0 \leq q^{1/3}$, we can bound the order of such subgroups. Then

$$\sum_{L \in \mathcal{L} \cap \mathcal{C}_5} \frac{1}{[H:L]} \leq \frac{1}{(q^2+q+1)(q^4+1)}.$$

For any f, there are at most 13 other subgroups in $\mathcal{L}$.

Then for all q

$$P_{G,G_0}(2) \geq 1 - \frac{14}{(q^2+q+1)(q^4+1)}.$$

□

5.3 Computational results

Throughout this section let G be an almost simple group with socle G_0 a classical group, and where G can be generated by 2 elements. Results from the previous section show that $P_{G,G_0}(2) \geq 0.927$ for nearly all classical groups. For the remaining classical groups we calculate either the exact value, or a lower bound for the probability $P_{G,G_0}(2)$ as described in Section 3.3. As mentioned previously, we exclude those groups with alternating socles. Using `EulerianFunction` in GAP [28] we calculate the exact value of the probability $P_{G,G_0}(2)$ for some almost simple groups whose socles are of the following types: $\mathrm{PSL}_2(q)$ for $q \leq 25$, $\mathrm{PSL}_3(q)$ for $q \leq 4$, $\mathrm{PSL}_4(3)$, $\mathrm{PSL}_5(2)$, $\mathrm{PSU}_3(3)$, $\mathrm{PSp}_4(3) \cong \mathrm{PSU}_4(2)$, $\mathrm{PSp}_4(4)$, $\mathrm{PSp}_4(5)$, $\mathrm{PSp}_6(2)$, $\mathrm{P\Omega}_8^+(2)$. In many of these cases we use the tables of marks in GAP [28, 74], as this makes our calculations much faster. The results of these calculations are displayed in Table 5.4 and Table 5.5.

In some cases we have not calculated the exact probability for all automorphism groups with these socles, as table of marks information was unavailable and the groups were too large to compute with otherwise. In these cases we find a lower estimate for their probability later.

For larger classical groups, we may estimate a lower bound for the probability. Let H be one of the quasisimple classical groups $\mathrm{SL}_n(q)$, $\mathrm{Sp}_n(q)$, $\mathrm{SU}_n(q)$, $\Omega_n(q)$, $\Omega_n^{\pm}(q)$ in dimension $n \leq 12$ and let G_0 be the corresponding simple group. The function `ClassicalMaximals` in Magma [8] allows us to obtain a set $\mathcal{L}$ of conjugacy class representatives for subgroups L of H where L is maximal or $L = M \cap H$, for M a novelty maximal subgroup of an extension K of H where $G_0 \leq K/Z(K) \leq \mathrm{Aut}(G_0)$. If $G_0 \leq G \leq \mathrm{Aut}(G_0)$ is 2-generated, then by Lemma 3.2.9,

$$P_{G,G_0}(2) \geq 1 - \sum_{L \in \mathcal{L}} \frac{1}{[H:L]}.$$

Then the probability for all possible G with a given socle G_0 can be estimated using Magma and the results of these calculations are given in Tables 5.6 and 5.7.

For a few almost simple groups, bounds calculated using the function `ClassicalMaximals` as described above, are not good enough to show that $P_{G,G_0}(2)$ is at least 0.927, as we are sometimes overestimating the sum

G	$G_0 = \mathrm{Soc}(G)$	$P_{G,G_0}(2)$	$P_{G,G_0}(2)$
$\mathrm{PSL}_2(7) \cong \mathrm{PSL}_3(2)$	$\mathrm{PSL}_2(7)$	19/28	0.678
$\mathrm{PGL}_2(7)$	$\mathrm{PSL}_2(7)$	23/28	0.821
$\mathrm{PSL}_2(8)$	$\mathrm{PSL}_2(8)$	71/84	0.845
$\mathrm{P\Gamma L}_2(8)$	$\mathrm{PSL}_2(8)$	71/84	0.845
$\mathrm{PSL}_2(11)$	$\mathrm{PSL}_2(11)$	127/165	0.769
$\mathrm{PGL}_2(11)$	$\mathrm{PSL}_2(11)$	146/165	0.884
$\mathrm{PSL}_2(13)$	$\mathrm{PSL}_2(13)$	165/182	0.906
$\mathrm{PGL}_2(13)$	$\mathrm{PSL}_2(13)$	165/182	0.906
$\mathrm{PSL}_2(16)$	$\mathrm{PSL}_2(16)$	313/340	0.920
$\mathrm{PSL}_2(16).2$	$\mathrm{PSL}_2(16)$	313/340	0.920
$\mathrm{P\Gamma L}_2(16)$	$\mathrm{PSL}_2(16)$	313/340	0.920
$\mathrm{PSL}_2(17)$	$\mathrm{PSL}_2(17)$	283/306	0.924
$\mathrm{PGL}_2(17)$	$\mathrm{PSL}_2(17)$	143/153	0.934
$\mathrm{PSL}_2(19)$	$\mathrm{PSL}_2(19)$	157/171	0.918
$\mathrm{PGL}_2(19)$	$\mathrm{PSL}_2(19)$	268/285	0.940
$\mathrm{PSL}_2(23)$	$\mathrm{PSL}_2(23)$	2881/3036	0.948
$\mathrm{PGL}_2(23)$	$\mathrm{PSL}_2(23)$	263/276	0.952
$\mathrm{PSL}_2(25)$	$\mathrm{PSL}_2(25)$	911/975	0.934
$\mathrm{PSL}_2(25).2_2$	$\mathrm{PSL}_2(25)$	911/975	0.934
$\mathrm{PGL}_2(25)$	$\mathrm{PSL}_2(25)$	311/325	0.956
$\mathrm{PSL}_2(25).2_3$	$\mathrm{PSL}_2(25)$	311/325	0.956
$\mathrm{P\Gamma L}_2(25)$	$\mathrm{PSL}_2(25)$	311/325	0.956

Table 5.4: Exact values for $P_{G,G_0}(2)$ for almost simple classical groups G, with socle $G_0 = \mathrm{PSL}_2(q)$

$\sum_{M \in \mathcal{M}} 1/[G : M]$ by including the intersection with H of any novelty maximal subgroup. In these remaining cases we can calculate the maximal subgroups of G using GAP or MAGMA or use the lists of maximal subgroups in the ATLAS [17] to estimate $P_{G,G_0}(2)$ using Lemma 3.2.6. These values are displayed in Table 5.8.

5.4 Probability bounds for almost simple classical groups

We now combine the results from previous sections to prove $P_{G,G_0}(2) \geq 53/90$ for almost simple classical groups G that can be generated by 2 elements. We also list the classical groups with the lowest values of $P_{G,G_0}(2)$. We consider each of the families of classical groups in turn.

Theorem 5.4.1. *Let G be an almost simple group with socle $G_0 = \mathrm{PSL}_n(q)$ which is not isomorphic to an alternating group. Suppose G can be generated*

G	$G_0 = \mathrm{Soc}(G)$	$P_{G,G_0}(2)$	$P_{G,G_0}(2)$
$\mathrm{PSL}_3(3)$	$\mathrm{PSL}_3(3)$	101/117	0.863
$\mathrm{PSL}_3(3).2$	$\mathrm{PSL}_3(3)$	113/117	0.965
$\mathrm{PSL}_3(4)$	$\mathrm{PSL}_3(4)$	121/140	0.864
$\mathrm{PGL}_3(4)$	$\mathrm{PSL}_3(4)$	3067/3360	0.912
$\mathrm{PSL}_3(4).2_1$	$\mathrm{PSL}_3(4)$	1541/1680	0.917
$\mathrm{PSL}_3(4).2_2$	$\mathrm{PSL}_3(4)$	4519/5040	0.896
$\mathrm{PSL}_3(4).2_3$	$\mathrm{PSL}_3(4)$	101/105	0.961
$\mathrm{PSL}_3(4).6$	$\mathrm{PSL}_3(4)$	3307/3360	0.984
$\mathrm{P\Gamma L}_3(4)$	$\mathrm{PSL}_3(4)$	3067/3360	0.912
$\mathrm{PSL}_3(4).3.2_3$	$\mathrm{PSL}_3(4)$	3307/3360	0.984
$\mathrm{PSL}_3(4).2^2$	$\mathrm{PSL}_3(4)$	101/105	0.961
$\mathrm{PSL}_3(4).D_{12}$	$\mathrm{PSL}_3(4)$	3307/3360	0.984
$\mathrm{PSU}_3(3)$	$\mathrm{PSU}_3(3)$	58/63	0.920
$\mathrm{PSU}_3(3).2$	$\mathrm{PSU}_3(3)$	11/12	0.916
$\mathrm{PSU}_3(5)$	$\mathrm{PSU}_3(5)$	19483/21000	0.927
$\mathrm{PSU}_3(5).2$	$\mathrm{PSU}_3(5)$	60919/63000	0.966
$\mathrm{PSU}_3(5).3$	$\mathrm{PSU}_3(5)$	6927/7000	0.989
$\mathrm{PSU}_3(5).S_3$	$\mathrm{PSU}_3(5)$	6927/7000	0.989
$\mathrm{PSL}_4(3)$	$\mathrm{PSL}_4(3)$	706709/758160	0.932
$\mathrm{PSp}_4(3) \cong \mathrm{PSU}_4(2)$	$\mathrm{PSp}_4(3) \cong \mathrm{PSU}_4(2)$	767/864	0.887
$\mathrm{PSp}_4(3).2 \cong \mathrm{PSU}_4(2).2$	$\mathrm{PSp}_4(3) \cong \mathrm{PSU}_4(2)$	767/864	0.887
$\mathrm{PSp}_4(4)$	$\mathrm{PSp}_4(4)$	116333/122400	0.950
$\mathrm{PSp}_4(4).2$	$\mathrm{PSp}_4(4)$	116333/122400	0.950
$\mathrm{PSp}_4(5)$	$\mathrm{PSp}_4(5)$	127669/130000	0.982
$\mathrm{PSL}_5(2)$	$\mathrm{PSL}_5(2)$	310801/333312	0.932
$\mathrm{PSp}_6(2)$	$\mathrm{PSp}_6(2)$	219703/241920	0.908
$\mathrm{P\Omega}_8^+(2)$	$\mathrm{P\Omega}_8^+(2)$	340661/358400	0.950

Table 5.5: Exact values for $P_{G,G_0}(2)$ for almost simple classical groups G, with socle G_0

by two elements. Then $P_{G,G_0}(2) \geq 19/28 > 0.678$. *Furthermore,* $P_{G,G_0}(2) \geq 0.927$ *except when* G_0 *is isomorphic to one of* $\mathrm{PSL}_2(7)$, $\mathrm{PSL}_2(8)$, $\mathrm{PSL}_2(11)$, $\mathrm{PSL}_2(13)$ *or* $\mathrm{PSL}_2(16)$, *or when* G *is isomorphic to one of* $\mathrm{PSL}_2(17)$, $\mathrm{PSL}_2(19)$, $\mathrm{PSL}_3(3)$, $\mathrm{PSL}_3(4)$, $\mathrm{PGL}_3(4)$, $\mathrm{PSL}_3(4).2_1$, $\mathrm{PSL}_3(4).2_2$ *or* $\mathrm{P\Gamma L}_3(4)$.

Proof. If $n \geq 5$ and $q \geq 2$, then Theorem 5.1.12, together with estimates from Tables 5.5, 5.6 and 5.8, shows that $P_{G,G_0}(2) \geq 0.927$.

If $n = 4$, Lemma 5.2.3 shows that $P_{G,G_0}(2) \geq 0.927$ for $q \geq 8$. Tables 5.5 and 5.6 show that the same bound holds for $q \geq 3$. We do not consider $q = 2$, as $\mathrm{PSL}_4(2) \cong A_8$.

If $n = 3$ and $q \geq 17$, Lemma 5.2.2 shows that $P_{G,G_0}(2) \geq 0.927$. Lower bounds calculated using Magma [8] show that the same bound holds for

$G_0 = \mathrm{Soc}(G)$	$P_{G,G_0}(2) >$	$G_0 = \mathrm{Soc}(G)$	$P_{G,G_0}(2) >$
$\mathrm{PSL}_2(27)$	0.957	$\mathrm{PSL}_3(16)$	0.992
$\mathrm{PSL}_2(29)$	0.951	$\mathrm{PSL}_4(4)$	0.971
$\mathrm{PSL}_2(31)$	0.953	$\mathrm{PSL}_4(5)$	0.984
$\mathrm{PSL}_2(32)$	0.965	$\mathrm{PSL}_4(7)$	0.994
$\mathrm{PSL}_2(37)$	0.970	$\mathrm{PSL}_5(3)$	0.981
$\mathrm{PSL}_2(41)$	0.968	$\mathrm{PSL}_5(4)$	0.993
$\mathrm{PSL}_2(43)$	0.974	$\mathrm{PSL}_6(2)$	0.963
$\mathrm{PSL}_3(5)$	0.927	$\mathrm{PSL}_6(3)$	0.994
$\mathrm{PSL}_3(7)$	0.961	$\mathrm{PSL}_7(2)$	0.983
$\mathrm{PSL}_3(8)$	0.970	$\mathrm{PSL}_8(2)$	0.991
$\mathrm{PSL}_3(9)$	0.976	$\mathrm{PSL}_9(2)$	0.996
$\mathrm{PSL}_3(11)$	0.984	$\mathrm{PSL}_{10}(2)$	0.998
$\mathrm{PSL}_3(13)$	0.988	$\mathrm{PSL}_{11}(2)$	0.999

Table 5.6: Lower bounds on the probability of generating almost simple classical groups G, with socle $G_0 = \mathrm{PSL}_n(q)$

$q \geq 5$ (Table 5.6). It remains to consider $G_0 = \mathrm{PSL}_3(2) \cong \mathrm{PSL}_2(7)$, $\mathrm{PSL}_3(3)$ and $\mathrm{PSL}_3(4)$. The values for $P_{G,G_0}(2)$ when G_0 is one of these 3 groups have been calculated exactly and are displayed in Table 5.4. In all these cases $P_{G,G_0}(2) > 0.678$, and we see precisely when $P_{G,G_0}(2) \geq 0.927$.

Finally consider the case where $n = 2$. Recall that $q \geq 4$ for G_0 to be simple. We exclude $q = 4, 5, 9$ as in these cases G_0 is isomorphic to an alternating group. Lemma 5.2.1 shows that $P_{G,G_0}(2) \geq 0.927$ for $q \geq 47$. Exact values for $P_{G,G_0}(2)$ when $4 \leq q \leq 25$ are displayed in Table 5.4, and lower bounds for $27 \leq q \leq 43$ are displayed in Table 5.6. Then we see that in all cases $P_{G,G_0}(2) > 0.678$, and $P_{G,G_0}(2) \geq 0.927$ except in the cases listed in the statement of the theorem. □

As $\mathrm{PSp}_2(q) \cong \mathrm{PSL}_2(q)$, and symplectic groups are only defined in even dimensions, we only consider $n \geq 4$ for the symplectic groups. We exclude $\mathrm{PSp}_4(2) = \mathrm{Sp}_4(2)$ as it is not simple, although $\mathrm{Sp}_4(2)' \cong \mathrm{PSL}_2(9) \cong A_6$ is. Probabilities for almost simple groups with socle A_6 have already been calculated.

Theorem 5.4.2. *Let G be an almost simple classical group with socle $G_0 = \mathrm{PSp}_n(q)$ for $n \geq 4$. Then $P_{G,G_0}(2) \geq 767/864 > 0.887$. If G_0 is not isomorphic to $\mathrm{PSp}_4(3)$ or $\mathrm{PSp}_6(2)$, then $P_{G,G_0}(2) \geq 0.927$.*

Proof. By Theorem 5.1.13, Lemma 5.2.6 and the calculations in Table 5.7, if $n \geq 8$ then $P_{G,G_0}(2) \geq 0.927$.

Lemma 5.2.5 shows that $P_{G,G_0}(2) \geq 0.927$ if $n = 6$ and $q \geq 3$, and Lemma 5.2.4 shows that $P_{G,G_0}(2) \geq 0.927$ for $n = 4$ and $q \geq 7$. As $\mathrm{PSp}_4(2)$

$G_0 = \mathrm{Soc}(G)$	$P_{G,G_0}(2) >$	$G_0 = \mathrm{Soc}(G)$	$P_{G,G_0}(2) >$
$\mathrm{PSU}_3(4)$	0.976	$\mathrm{PSU}_7(11)$	0.999
$\mathrm{PSU}_4(3)$	0.949	$\mathrm{PSU}_7(13)$	0.999
$\mathrm{PSU}_4(4)$	0.994	$\mathrm{PSp}_8(2)$	0.979
$\mathrm{PSU}_5(2)$	0.983	$\mathrm{PSU}_8(2)$	0.999
$\mathrm{PSU}_7(2)$	0.999	$\mathrm{P}\Omega_8^-(2)$	0.981
$\mathrm{PSU}_7(3)$	0.999	$\Omega_9(3)$	0.999
$\mathrm{PSU}_7(4)$	0.999	$\Omega_9(5)$	0.999
$\mathrm{PSU}_7(5)$	0.999	$\mathrm{P}\Omega_{10}^+(2)$	0.995
$\mathrm{PSU}_7(7)$	0.999	$\mathrm{P}\Omega_{10}^+(3)$	0.999
$\mathrm{PSU}_7(8)$	0.999	$\mathrm{P}\Omega_{10}^-(2)$	0.995
$\mathrm{PSU}_7(9)$	0.999	$\mathrm{P}\Omega_{10}^-(3)$	0.999

Table 5.7: Lower bounds on the probability of generating almost simple classical groups G, with socle G_0

G	$\mathrm{Soc}(G) = G_0$	$P_{G,G_0}(2) \geq$
$\mathrm{PGL}_4(3)$	$\mathrm{PSL}_4(3)$	0.941
$\mathrm{PSL}_4(3).2_2$	$\mathrm{PSL}_4(3)$	0.971
$\mathrm{PSL}_4(3).2_3$	$\mathrm{PSL}_4(3)$	0.988
$\mathrm{PSL}_4(3).2^2$	$\mathrm{PSL}_4(3)$	0.988
$\mathrm{PSp}_4(4).4$	$\mathrm{PSp}_4(4)$	0.996
$\mathrm{PSp}_4(5).2$	$\mathrm{PSp}_4(5)$	0.980
$\mathrm{PSL}_5(2).2$	$\mathrm{PSL}_5(2)$	0.994
$\mathrm{P}\Omega_8^+(2).2$	$\mathrm{P}\Omega_8^+(2)$	0.981
$\mathrm{P}\Omega_8^+(2).3$	$\mathrm{P}\Omega_8^+(2)$	0.999
$\mathrm{P}\Omega_8^+(2).S_3$	$\mathrm{P}\Omega_8^+(2)$	0.999

Table 5.8: Lower bounds on the probability of generating some almost simple classical groups G, with socle G_0

is not simple, it remains to consider the cases where $G_0 = \mathrm{PSp}_4(3)$, $\mathrm{PSp}_4(4)$, $\mathrm{PSp}_4(5)$ or $\mathrm{PSp}_6(2)$.

If $G_0 = \mathrm{PSp}_4(3)$, either $G = \mathrm{PSp}_4(3)$ or $G = \mathrm{Aut}(\mathrm{PSp}_4(3))$. We calculate the exact probabilities using GAP and see that in both cases $P_{G,G_0}(2) = 767/864 > 0.887$ (Table 5.5).

If $G_0 = \mathrm{PSp}_4(4)$, the possibilities for G are $\mathrm{PSp}_4(4)$, $\mathrm{PSp}_4(4).2$ and $\mathrm{PSp}_4(4).4$. When $G = \mathrm{PSp}_4(4)$ or $\mathrm{PSp}_4(4).2$, we calculate the exact probability using GAP and these values are displayed in Table 5.5. In both these cases $P_{G,G_0}(2) \geq 0.927$. When $G = \mathrm{PSp}_4(4).4$ we use maximal subgroup information from the Atlas to estimate the probability and see that in this case too, $P_{G,G_0}(2) \geq 0.927$. If $G_0 = \mathrm{PSp}_4(5)$, then $G = \mathrm{PSp}_4(5)$ or $\mathrm{PSp}_4(5).2$. In the first case the exact value for $P_{G,G_0}(2)$ is given in Table

5.5, otherwise the lower bound is in Table 5.8.

Finally, if $G_0 = \mathrm{PSp}_6(2)$, $\mathrm{Out}(G_0) = 1$ and so the only possibility for G is $G = G_0$. We calculate the exact probability using GAP (Table 5.5) and obtain $P_{G_0}(2) = 219703/241920 > 0.908$.

In summary, $P_{G,G_0}(2) > 0.887$, and if $G_0 \neq \mathrm{PSp}_4(3)$ or $\mathrm{PSp}_6(2)$ then $P_{G,G_0}(2) \geq 0.927$. □

Next we consider $G_0 = \mathrm{PSU}_n(q)$. We need only consider $n \geq 3$ as $\mathrm{PSU}_2(q) \cong \mathrm{PSL}_2(q)$.

Theorem 5.4.3. *Let G be an almost simple group with socle $G_0 = \mathrm{PSU}_n(q)$, for $n \geq 3$. Then $P_{G,G_0}(2) \geq 767/864 > 0.887$. If $G_0 \neq \mathrm{PSU}_3(3)$ or $\mathrm{PSU}_4(2)$ then $P_{G,G_0}(2) \geq 0.927$.*

Proof. By Theorem 5.1.14 if $n \geq 9$, if $n \geq 8$ and $q \geq 3$, or if $n \geq 7$ and $q \geq 16$, then $P_{G,G_0}(2) \geq 0.927$. Computational estimates (Table 5.7) show that this bound also holds if $G_0 = \mathrm{PSU}_8(2)$ or $\mathrm{PSU}_7(q)$ for $q \leq 13$.

It remains to show that the bounds on $P_{G,G_0}(2)$ hold when $3 \leq n \leq 6$. Lemma 5.2.10, shows that $P_{G,G_0}(2) \geq 0.927$ if $n = 6$. When $n = 5$ Lemma 5.2.9 shows that $P_{G,G_0}(2) \geq 0.927$ for $q \geq 3$. Table 5.7 shows that the same lower bound holds when $G_0 = \mathrm{PSU}_5(2)$.

Lemma 5.2.8 and calculations from Table 5.7 show that $P_{G,G_0}(2) \geq 0.927$ if $n = 4$ and $q \geq 3$. If $G_0 = \mathrm{PSU}_4(2)$, either $G = \mathrm{PSU}_4(2)$, or $G = \mathrm{Aut}(G_0)$. For these cases we calculate the exact probability in GAP as shown in Table 5.5, and we see that $P_{G,G_0}(2) = 767/864$ for both possibilities for G.

By Lemma 5.2.7, when $n = 3$ and $q \geq 7$, then $P_{G,G_0}(2) \geq 0.927$. Tables 5.5 and 5.7 show that the same lower bound holds when $G_0 = \mathrm{PSU}_3(4)$ or $\mathrm{PSU}_3(5)$. Finally if $G_0 = \mathrm{PSU}_3(3)$, then $P_{\mathrm{PSU}_3(3).3,\mathrm{PSU}_3(3)}(2) > 0.916$ and $P_{\mathrm{PSU}_3(3)}(2) > 0.920$. □

Theorem 5.4.4. *Let G be an almost simple group with socle $G_0 = \Omega_n(q)$ for $n \geq 7$, and nq odd. Then $P_{G,G_0}(2) \geq 0.927$.*

Proof. In this case n and q are both odd. By Theorem 5.1.15, if $n \geq 11$, or if $n \geq 9$ and $q \geq 7$ then $P_{G,G_0}(2) \geq 0.927$. Lemmas 5.2.11 and Table 5.7 shows that this bound also holds for the remaining values of n and q. □

Theorem 5.4.5. *Let G be an almost simple group with socle $G_0 = \mathrm{P}\Omega_n^+(q)$ where $n \geq 8$ and where G can be generated by 2 elements. Then $P_{G,G_0}(2) \geq 0.927$.*

Proof. By Theorem 5.1.16 and estimates in Table 5.7, $P_{G,G_0}(2) \geq 0.927$ for $n \geq 10$.

If $n = 8$ and $q \geq 3$, then by Lemma 5.2.12, $P_{G,G_0}(2) \geq 0.927$. When $G_0 = \mathrm{P}\Omega_8^+(2)$, the possibilities for G are: $\mathrm{P}\Omega_8^+(2)$, $\mathrm{P}\Omega_8^+(2).2$, $\mathrm{P}\Omega_8^+(2).3$, $\mathrm{P}\Omega_8^+(2).S_3$. If $G = \mathrm{P}\Omega_8^+(2)$ the probability has been calculated exactly

(Table 5.5). For the remaining 3 possibilities for G, maximal subgroup information is available in the ATLAS and we use this to estimate $P_{G,G_0}(2)$. We see from Table 5.8 that $P_{G,G_0}(2) \geq 0.927$ in the remaining cases. □

Theorem 5.4.6. *Let G be an almost simple group with socle $G_0 = \mathrm{P}\Omega_n^-(q)$, where $n \geq 8$. Then $P_{G,G_0}(2) \geq 0.927$.*

Proof. Theorem 5.1.17 shows that if $n \geq 12$, or if $n = 10$ and $q \geq 4$, then $P_{G,G_0}(2) \geq 0.927$. Estimates calculated using MAGMA (Table 5.7) shows that the same bound holds when $G_0 = \mathrm{P}\Omega_{10}^-(2)$ or $\mathrm{P}\Omega_{10}^-(3)$. If $n = 8$, then Lemma 5.2.13 shows that $P_{G,G_0}(2) \geq 0.927$ for $q \geq 3$. When $G_0 = \mathrm{P}\Omega_8^-(q)$, the same lower bound holds by calculations displayed in Table 5.7. □

Combining Theorems 5.4.1 – 5.4.6 completes the proof of Theorem 5.0.1 and bounds $P_{G,G_0}(2)$ for almost simple classical groups G.

Chapter 6

The probability of generating an exceptional group

Let $G_0 \leq G \leq \mathrm{Aut}(G_0)$ for a simple exceptional group G_0. Recall that all such groups G may be generated by 2 elements, and so we may consider $P_{G,G_0}(2)$. In this chapter we prove the following theorem.

Theorem 6.0.1. *Let G be an almost simple group with socle G_0 an exceptional group. Then $P_{G,G_0}(2) > 0.931$.*

For each family of exceptional groups, where the families are as described in Section 2.3, we obtain explicit lower bounds for $P_{G,G_0}(2)$ in terms of q. Using Lemma 3.2.6 we do this by estimating the index and number of maximal subgroups of G not containing G_0. We would like to use the estimates from [40] and [62] to estimate $P_{G,G_0}(2)$.

Full maximal subgroup information is available when G_0 is one of the following: ${}^2\mathrm{B}_2(q)$, $\mathrm{G}_2(q)$, ${}^2\mathrm{G}_2(q)$, ${}^3\mathrm{D}_4(q)$, and ${}^2\mathrm{F}_4(q)$. In these cases an estimate for $P_{G,G_0}(2)$ is straightforward to calculate. The remaining cases ($G_0 = \mathrm{F}_4(q)$, $\mathrm{E}_6(q)$, ${}^2\mathrm{E}_6(q)$, $\mathrm{E}_7(q)$ and $\mathrm{E}_8(q)$) are considered in [62] and probability estimates are obtained for each family of groups in terms of q. These estimates use unspecified constants, as their result is concerned with the behaviour as $|G| \to \infty$. By looking at the proof in more detail we may calculate the constants, but these bounds are not quite good enough to show $P_{G,G_0}(2) \geq 53/90$, for all q. For the remaining values of q, the groups are too large to compute with, and in most cases full maximal subgroup information is not available.

To bound $P_{G,G_0}(2)$ for $G_0 = \mathrm{F}_4(q)$, $\mathrm{E}_6(q)$, ${}^2\mathrm{E}_6(q)$, $\mathrm{E}_7(q)$ or $\mathrm{E}_8(q)$, we follow the proof in [62], but are more careful with all our estimates and keep track of all constants. The idea of the proof is as follows. As in [62] we split the maximal subgroups of G into two sets: the 'known' subgroups $\mathcal{K}$, and the 'unknown' subgroups $\mathcal{U}$. Subgroups in $\mathcal{K}$ are known up to conjugacy, and there are only a small number of these. The remaining subgroups in $\mathcal{U}$

are almost simple, and we have an upper bound on their order. In this case the number of subgroups is not known. We use the fact that every finite simple group can be generated by an involution and another element to find a rough upper bound on the number of subgroups in $\mathcal{U}$. For some small G_0 ($G_0 = \mathrm{F}_4(q)$ for $q \leq 17$ and $\mathrm{E}_6(q)$ or ${}^2\mathrm{E}_6(q)$ for $q \leq 3$), these probability bounds are not quite good enough, and we consider these groups separately. In these cases for a specified q there are a limited number of possibilities for the socles of maximal subgroups in $\mathcal{U}$. As these groups are smaller, we can compute with the socles of maximal subgroups in $\mathcal{U}$, and obtain tighter bounds on their order. We also obtain good estimates in the cases $G_0 = \mathrm{F}_4(2)$, $\mathrm{E}_6(2)$, and ${}^2\mathrm{E}_6(2)$, as their maximal subgroups are known.

6.1 Small rank exceptional groups

Let $G_0 = X(q)$ for $X \in \{{}^2\mathrm{B}_2(q), {}^2\mathrm{G}_2(q), \mathrm{G}_2(q), {}^3\mathrm{D}_4(q), {}^2\mathrm{F}_4(q)\}$, let $q = p^n$ for some prime p, and suppose G_0 is simple. Orders of these groups G_0 and descriptions of their outer automorphism groups are given in Section 2.3. Let G be an almost simple group with socle G_0. Then let $\mathcal{L}$ be a set of conjugacy class representatives in G_0 for subgroups $M \cap G_0$, where M is a max subgroup of G, and $G_0 \leq M$. This set $\mathcal{L}$ is known, and we estimate $P_{G,G_0}(2)$ using Lemma 3.2.7. In each case some of our subgroups $M \cap G_0$ are of the form $X(q_0)$, where $q = q_0^\alpha$ for some prime α. We get at most one conjugacy class in G_0 for each prime α, that is, there is one conjugacy class for each prime divisor of n. Then the number of conjugacy classes is bounded by $\log n \leq \log \log q$. If n is odd, then all divisors of n must be odd and at least 3. Then in this case, the number of prime divisors of n is at most $\log_3 n$.

First consider the case $G_0 = {}^2\mathrm{B}_2(q)$. Here $q = 2^{2m+1}$ for some $m \geq 0$. As ${}^2\mathrm{B}_2(2)$ is not simple we are only interested in the case where $q \geq 8$.

Theorem 6.1.1 ([86, Theorem 9, Theorem 10])**.** *The group ${}^2\mathrm{B}_2(q)$ contains the following subgroups:*

1. *H, a Frobenius group of order $q^2(q-1)$,*
2. *B_0, a dihedral group of order $2(q-1)$,*
3. *A_i, a cyclic group of order $q \pm \sqrt{2q} + 1$ $(i = 1, 2)$,*
4. *B_i, the normaliser $N_G(A_i)$ with order $4(q \pm \sqrt{2q} + 1)$ $(i = 1, 2)$,*
5. *${}^2\mathrm{B}_2(q_0)$, if $q = q_0^\alpha$ for some α.*

Conversely, any subgroup of ${}^2\mathrm{B}_2(q)$ is either conjugate to ${}^2\mathrm{B}_2(q_0)$ for some q_0 such that $q_0^\alpha = q$, or conjugate in ${}^2\mathrm{B}_2(q)$ to a subgroup of H or B_i $(i = 0, 1, 2)$.

Lemma 6.1.2. *Let G be an almost simple group with socle $G_0 = {}^2\mathrm{B}_2(q)$ with $q = 2^{2m+1}$ for $m \geq 1$. Then*

$$P_{G,G_0}(2) \geq 1 - \frac{4}{q^2} - \frac{\log\log q}{q^3}$$

and $P_{G,G_0}(2) > 0.931$.

Proof. The order of G_0 is $q^2(q^2+1)(q-1)$ as given in Table 2.8. Let $\mathcal{L}$ be the set of subgroups H, B_0, B_1, B_2, or ${}^2\mathrm{B}_2(q_0)$ for $q = q_0^\alpha$, for some α, as described in Theorem 6.1.1. By [10], there are no novelty maximal subgroups. Then for all maximal subgroups of M of G, the subgroup $L = M \cap G_0$ is conjugate in G_0 to one of the subgroups in $\mathcal{L}$. So by Lemma 3.2.7 $P_{G,G_0}(q) \geq 1 - \sum_{L\in\mathcal{L}} 1/[G_0 : L]$.

Subgroups of the form H or B_i have index at least q^2 in G_0 and there is one class of each up to conjugacy in G_0. If L is a subgroup of the form ${}^2\mathrm{B}_2(q_0)$ with $q_0^\alpha = q$, then as α must be odd $q_0 \leq q^{1/3}$. Subgroups of this form have index at least q^3, and there are at most $\log\log q$ of them up to conjugacy. Then

$$\sum_{L\in\mathcal{L}} \frac{1}{[G_0 : L]} \leq \frac{4}{q^2} + \frac{\log\log q}{q^3} \text{ and so } P_{G,G_0}(2) \geq 1 - \frac{4}{q^2} - \frac{\log\log q}{q^3}.$$

This estimate increases with increasing q and as $q \geq 8$ the probability is bounded by $P_{G,G_0}(2) > 0.931$. □

Next consider $G_0 = \mathrm{G}_2(q)$. This is simple if and only if $q \geq 3$. We consider the cases where q is even and q is odd separately.

Theorem 6.1.3 ([19, Theorem 2.3])**.** *Let $G_0 = \mathrm{G}_2(q)$, $q = 2^n$ with $n > 2$. Conjugacy class representatives for maximal subgroups of G_0 are as follows.*

1. *P_a, a subgroup of order $q^6(q-1)(q^2-1)$,*
2. *P_b, a subgroup of order $q^6(q-1)(q^2-1)$,*
3. *$\mathrm{SL}_3(q) : 2$,*
4. *$\mathrm{SU}_3(q) : 2$,*
5. *$\mathrm{SL}_2(q) \times \mathrm{SL}_2(q)$,*
6. *$\mathrm{G}_2(q_0)$, where $q_0 = 2^m$ for n/m prime.*

Lemma 6.1.4. *Let G be an almost simple group with socle $G_0 = \mathrm{G}_2(q)$ for $q = 2^n$. Then*

$$P_{G,G_0}(2) \geq 1 - \frac{5}{q^5} - \frac{\log\log q}{q^7}$$

and $P_{G,G_0}(G) > 0.995$.

Proof. The order of G_0 is $q^6(q^2-1)(q^6-1)$. Let $\mathcal{L}$ be a set of conjugacy class representatives in G_0 for subgroups $L = M \cap G_0$, where M is an ordinary or novelty maximal subgroup of G. Then we estimate $\sum_{L\in\mathcal{L}} 1/[G_0 : L]$, and use Lemmas 3.2.6 and 3.2.7 to estimate $P_{G,G_0}(2)$.

First suppose $n \geq 3$ and so $q \geq 8$. Conjugacy classes of maximal subgroups of G_0 are listed in Theorem 6.1.3, and by [10] we know that we do not get any novelty maximal subgroups of G. Then the possibilities for $\mathcal{L}$ are those subgroups listed in Theorem 6.1.3. We get a maximal subgroup of G_0 of the form $\mathrm{G}_2(2^m)$ for every prime divisor of n. The number of prime divisors of n is bounded above by $\log n \leq \log\log q$ and the index of such a subgroup is greater than q^7. There are at most 5 other maximal subgroups of G_0 up to conjugacy. The subgroups with minimal index are P_a and P_b. These have index at least q^5. Then for $q \geq 8$,

$$\sum_{L\in\mathcal{L}} \frac{1}{[G_0 : L]} \leq \frac{5}{q^5} + \frac{\log\log q}{q^7}.$$

This estimate is increasing with increasing q and so if $q \geq 8$ then $P_{G,G_0}(2) \geq 0.999$.

If $q = 4$ then $G = \mathrm{G}_2(4)$ or $\mathrm{Aut}(\mathrm{G}_2(4)) = \mathrm{G}_2(4).2$. Using GAP we calculate the exact probability when $G = \mathrm{G}_2(4)$. The maximal subgroups of $\mathrm{G}_2(4).2$ are available in [19] and so we calculate a lower bound for the probability in this case. In both cases $P_{G,\mathrm{G}_2(4)}(2) > 0.995$ and for $q = 4$, $P_{G,G_0}(2) \geq 1 - 5/q^5 - (\log\log q)/q^7$. □

Next we consider $G_0 = \mathrm{G}_2(q)$ where $q = p^n$ for some odd prime p. If $p = 3$ then $\mathrm{Aut}(G_0)$ may contain a graph automorphism, otherwise $\mathrm{Aut}(G_0)$ is the group of inner and field automorphisms of G_0. Both these cases are considered in the two following theorems.

Theorem 6.1.5 ([43, Theorem A])**.** *Assume that $G_0 \leq G \leq \mathrm{Aut}(G_0)$ where $G_0 = \mathrm{G}_2(q)$ and $q = p^n$ is odd. Further suppose $\mathrm{Aut}(G_0)$ does not contain a graph automorphism of G_0. Let M be a maximal subgroup of G not containing G_0. Then $M_0 = M \cap G_0$ is G_0-conjugate to one of the following groups:*

1. $[q^5] : \mathrm{GL}_2(q)$ *(2 classes),*
2. $(\mathrm{SL}_2(q) \circ \mathrm{SL}_2(q)).2$*,*
3. $2^{3\cdot}\mathrm{PSL}_3(2)$ *if $q = p$,*
4. $\mathrm{SL}_3(q) : 2$ *(2 classes if $p = 3$, 1 class otherwise),*
5. $\mathrm{SU}_3(q) : 2$ *(2 classes if $p = 3$, 1 class otherwise),*
6. $\mathrm{G}_2(q_0)$ *if $q = q_0^\alpha$ for α prime,*

7. ${}^2\mathrm{G}_2(q)$ *if* $p = 3$ *and* n *odd,*

8. $\mathrm{PGL}_2(q)$ *if* $p \geq 7$ *and* $q \geq 11$,

9. $\mathrm{PSL}_2(8)$ *if* $p \geq 5$ *and* $\mathbb{F}_q = \mathbb{F}_p[\omega]$, *where* $\omega^3 - 3\omega + 1 = 0$,

10. $\mathrm{PSL}_2(13)$ *if* $p \neq 13$, $\mathbb{F}_q = \mathbb{F}_p[\sqrt{13}]$,

11. $\mathrm{G}_2(2)$ *if* $q = p \geq 5$,

12. J_1 *if* $q = 11$.

Conversely, if $K \leq G_0$ *is* G_0*-conjugate to one of these groups, then* $N_G(K)$ *is maximal in* G.

Theorem 6.1.6 ([43, Theorem B])**.** *Assume that* $G_0 \leq G \leq \mathrm{Aut}(G_0)$ *where* $G_0 = \mathrm{G}_2(q)$, $q = 3^n$ *and* G *contains a graph automorphism of* G_0. *Let* M *be a maximal subgroup of* G *not containing* G_0. *Then* $M_0 = M \cap G_0$ *is* G_0*-conjugate to one of the following groups:*

1. $[q^6] : \mathbb{Z}_{q-1}^2$,

2. $(\mathrm{SL}_2(q) \circ \mathrm{SL}_2(q)) \cdot 2$,

3. $2^{3\cdot}\mathrm{PSL}_3(2)$ *if* $q = 3$,

4. $(\mathbb{Z}_{q-1})^2.D_{12}$ *if* $q \geq 9$,

5. $(\mathbb{Z}_{q+1})^2.D_{12}$ *if* $q \geq 9$,

6. $\mathbb{Z}_{q^2+q+1}.\mathbb{Z}_6$ *if* $q \geq 9$,

7. $\mathbb{Z}_{q^2-q+1}.\mathbb{Z}_6$ *if* $q \geq 9$,

8. $\mathrm{G}_2(q_0)$ *if* $q = q_0^\alpha$, α *prime,*

9. ${}^2\mathrm{G}_2(q)$ *if* n *odd,*

10. $\mathrm{PSL}_2(13)$ *if* $q = 3$.

Conversely, if $K \leq G_0$ *is* G_0*-conjugate to one of these groups, then* $N_G(K)$ *is maximal in* G.

Lemma 6.1.7. *Let* G *be an almost simple group with socle* $G_0 = \mathrm{G}_2(q)$ *for* q *odd. Then*

$$P_{G,G_0}(2) \geq 1 - \frac{11}{q^4} - \frac{\log\log q}{q^7}$$

and $P_{G,G_0}(G) > 0.982$.

Proof. The order of G_0 is $q^6(q^2-1)(q^6-1)$. Let $\mathcal{L}$ be a set of conjugacy class representatives in G_0 for subgroups $L = M \cap G_0$, where M is an ordinary or novelty maximal subgroup of G. Then we estimate $\sum_{L\in\mathcal{L}} 1/[G_0 : L]$, and use Lemmas 3.2.6 and 3.2.7 to estimate $P_{G,G_0}(2)$.

Then $\mathcal{L}$ is the set of subgroups listed in Theorem 6.1.5 or Theorem 6.1.6. If $q = p^n$ the number of subgroups the form $\mathrm{G}_2(q_0) \in \mathcal{L}$ is the number of prime divisors of n. This is bounded above by $\log n \leq \log\log q$. The order of $\mathrm{G}_2(q_0)$ is $q_0^6(q_0^2-1)(q_0^6-1)$. As $q_0 \leq q^{1/2}$, the order can be bounded by $|\mathrm{G}_2(q_0)| \leq q^3(q-1)(q^3-1)$. The index of such a subgroup is $[G_0 : \mathrm{G}_2(q_0)] \geq q^7$ and there are at most $\log\log q$ such subgroups up to conjugacy. Taking into account that different subgroups occur for different values of q, there are at most 11 other maximal subgroups up to conjugacy. The index of a subgroup is bounded by $[G_0 : ([q^5] : \mathrm{GL}_2(q))] \geq q^4$. Then

$$\sum_{L\in\mathcal{L}} \frac{1}{[G_0 : L]} \leq \frac{11}{q^4} + \frac{\log\log q}{q^7}.$$

Thus for all q,

$$P_{G,G_0}(2) \geq 1 - \frac{11}{q^4} - \frac{\log\log q}{q^7}.$$

As this sum is increasing with increasing q, then if $q \geq 5$, $P_{G,G_0}(2) > 0.996$. When $q = 3$ the possiblities for G are $G = \mathrm{G}_2(3)$ or $G = \mathrm{Aut}(\mathrm{G}_2(3)) = \mathrm{G}_2(3).2$. In both these cases exact probabilities have been calculated using GAP and $P_{G,G_0}(2) > 0.983 \geq 1 - 11/q^4 - (\log\log q)/q^7$ when $q = 3$. The result follows. □

Next we consider $G_0 = {}^2\mathrm{G}_2(q)$. Here $q = 3^{2m+1}$ and we consider $q > 3$ as ${}^2\mathrm{G}_2(3)$ is not simple.

Theorem 6.1.8 ([43, Theorem C])**.** *Let $q = 3^{2m+1}$, and assume that $G_0 \leq G \leq \mathrm{Aut}(G_0)$, where $G_0 = {}^2\mathrm{G}_2(q)$. If M is a maximal subgroup of G not containing G_0, then $M_0 = M \cap G_0$ is G_0-conjugate to one of the following groups:*

1. $[q^3] : \mathbb{Z}_{q-1}$,
2. $2 \times \mathrm{PSL}_2(q)$ *if* $q \geq 27$,
3. $(2^2 \times D_{(q+1)}) : 3$ *if* $q \geq 27$,
4. $2^3 : 7 : 3$ *if* $q = 3$,
5. $\mathbb{Z}_{q+\sqrt{3q}+1} : \mathbb{Z}_6$,
6. $\mathbb{Z}_{q-\sqrt{3q}+1} : \mathbb{Z}_6$ *if* $q \geq 27$,
7. ${}^2\mathrm{G}_2(q_0)$ *if* $q = q_0^\alpha$ *and* α *prime,*

8. $\mathrm{PSL}_2(8)$ *if* $q = 3$.

Conversely, if $K \leq G_0$ *is* G_0 *conjugate to one of these groups then* $N_G(K)$ *is maximal in* G.

Lemma 6.1.9. *Let* G *be an almost simple group with socle* $G_0 = {}^2\mathrm{G}_2(q)$, *where* $q = 3^{2m+1}$. *Then*

$$P_{G,G_0}(2) \geq 1 - \frac{5}{q^2} - \frac{\log\log q}{q^4}$$

and $P_{G,G_0}(2) > 0.993$.

Proof. The order of G_0 is $q^3(q^3+1)(q-1)$. Let $\mathcal{L}$ be the set of subgroups listed in Theorem 6.1.8. Then we estimate $\sum_{L\in\mathcal{L}} 1/[G_0 : L]$ and use Lemmas 3.2.6 and Lemma 3.2.7 to estimate $P_{G,G_0}(2)$.

There is a subgroup of the form ${}^2\mathrm{G}_2(q_0) \in \mathcal{L}$ for each q_0 such that $q_0^\alpha = q$ for some odd prime α. The number of such subgroups is then bounded by the number of prime divisors of $2m+1$, which is itself bounded by $\log q$. As $q_0 \leq q^{1/3}$, the order of such a subgroup is bounded above by $q(q+1)(q^{1/3}-1)$ and so the index of such a subgroup in G_0 is bounded below by q^4. There are at most 5 other subgroups in $\mathcal{L}$, each of index at least q^2. Then $\sum_{L\in\mathcal{L}} 1/[G_0 : L] \leq 5/q^2 + (\log\log q)/q^4$ and so

$$P_{G,G_0}(2) \geq 1 - \frac{5}{q^2} - \frac{\log\log q}{q^4}.$$

This is increasing with increasing q and so $P_{G,G_0}(2) > 0.993$. □

Now consider almost simple groups with socles ${}^3\mathrm{D}_4(q)$.

Theorem 6.1.10 ([42])**.** *Let* $G_0 \leq G \leq \mathrm{Aut}(G_0)$ *for* $G_0 = {}^3\mathrm{D}_4(q)$ *and let* M *be a maximal subgroup of* G *not containing* G_0. *Then* $M_0 = M \cap G_0$ *is* G_0*-conjugate to one of the following groups:*

1. $[q^9] : (\mathrm{SL}_2(q^3) \circ \mathbb{Z}_{q-1}).d$ *where* $d = (2, q-1)$,
2. $[q^{11}] : (\mathbb{Z}_{q^3-1} \circ \mathrm{SL}_2(q)).d$ *where* $d = (2, q-1)$,
3. $\mathrm{G}_2(q)$,
4. $\mathrm{PGL}_3(q)$ *if* $q \equiv 1 \mod 3$,
5. $\mathrm{PGU}_3(q)$ *if* $q \equiv -1 \mod 3$ *and* $q > 2$,
6. ${}^3\mathrm{D}_4(q_0)$ *if* $q = q_0^\alpha$, α *prime,* $\alpha \neq 3$,
7. $\mathrm{PSL}_2(q^3) \times \mathrm{PSL}_2(q)$ *if* $p = 2$,
8. $(\mathrm{SL}_2(q^3) \circ \mathrm{SL}_2(q^3)).2$ *if* p *is odd,*

9. $(\mathbb{Z}_{q^2+q+1} \circ \mathrm{SL}_3(q)).(3, q^2+q+1).2$,

10. $(\mathbb{Z}_{q^2-q+1} \circ \mathrm{SU}_3(q)).(3, q^2-q+1).2$,

11. $(\mathbb{Z}_{q^2+q+1})^2.\mathrm{SL}_2(3)$,

12. $(\mathbb{Z}_{q^2-q+1})^2.\mathrm{SL}_2(3)$,

13. $(\mathbb{Z}_{q^4-q^2+1}).4$.

Conversely, if $K \leq G_0$ is G_0-conjugate to one of these groups then $N_G(K)$ is maximal in G.

Lemma 6.1.11. *Let G be an almost simple group with socle $G_0 = {}^3\mathrm{D}_4(q)$. Then*

$$P_{G,G_0}(2) \geq 1 - \frac{10}{q^8} - \frac{\log\log q}{q^{13}}$$

and $P_{G,G_0}(2) > 0.960$.

Proof. The order of G_0 is $q^{12}(q^8+q^4+1)(q^6-1)(q^2-1)$ (Table 2.8). Let $\mathcal{L}$ be the subgroups of G_0 listed in Theorem 6.1.10. By Lemmas 3.2.6 and 3.2.7,

$$P_{G,G_0}(2) \geq 1 - \sum_{L \in \mathcal{L}} \frac{1}{[G_0 : L]}.$$

There are at most $\log\log q$ subgroups of the form ${}^3\mathrm{D}_4(q_0)$ in $\mathcal{L}$, and each has index at least q^{13} (as $q_0 \leq q^{1/2}$). There are at most 10 other subgroups in $\mathcal{L}$. The subgroup with minimal index is $[q^9] : (\mathrm{SL}_2(q^3) \circ \mathbb{Z}_{q-1}).d$, which has index greater than q^8. Then

$$P_{G,G_0}(2) \geq 1 - \sum_{L \in \mathcal{L}} \frac{1}{[G_0 : L]} \geq 1 - \frac{10}{q^8} - \frac{\log\log q}{q^{13}}.$$

This is increasing with increasing q and so $P_{G,G_0}(2) > 0.960$. □

Finally we consider $G_0 = {}^2\mathrm{F}_4(q)$. In this case $q = 2^{2m+1}$, and G_0 is simple if and only if $q \geq 8$.

Theorem 6.1.12 ([68])**.** *Every maximal subgroup of ${}^2\mathrm{F}_4(q)$, $q = 2^{2m+1}$, $m \geq 1$, is conjugate to one of the following:*

1. $[q^{11}] : (\mathrm{PSL}_2(q) \times (q-1))$,

2. $[q^{10}] : ({}^2\mathrm{B}_2(q) \times (q-1))$,

3. $\mathrm{SU}_3(q) : 2$,

4. $(\mathbb{Z}_{q+1} \times \mathbb{Z}_{q+1}) : \mathrm{GL}_2(3)$,

5. $(\mathbb{Z}_{q-\sqrt{2q}+1} \times \mathbb{Z}_{q-\sqrt{2q}+1}) : [96]$ *if* $q > 8$,

6. $(\mathbb{Z}_{q+\sqrt{2q}+1} \times \mathbb{Z}_{q+\sqrt{2q}+1}) : [96]$,

7. $(\mathbb{Z}_{q^2-\sqrt{2q^3}+q-\sqrt{2q}+1}) : [12]$,

8. $(\mathbb{Z}_{q^2+\sqrt{2q^3}+q+\sqrt{2q}+1}) : [12]$,

9. $\mathrm{PGU}_3(q) : 2$,

10. ${}^2\mathrm{B}_2(q) \operatorname{wr} 2$,

11. $\mathrm{B}_2(q) : 2$,

12. ${}^2\mathrm{F}_4(q_0)$, *if* $q_0 = 2^{2k+1}$ *with* $\frac{2m+1}{2k+1}$ *prime.*

Conversely, there is exactly one class of maximal subgroups of ${}^2\mathrm{F}_4(q)$ *for each entry in the list.*

As described in [68], groups G such that ${}^2\mathrm{F}_4(q) \leq G \leq \mathrm{Aut}({}^2\mathrm{F}_4(q))$ are all extensions of ${}^2\mathrm{F}_4(q)$ by field automorphisms, that is, $G = {}^2\mathrm{F}_4(q) : f$ for $f|(2m+1)$. Then we determine maximal subgroups of almost simple groups G.

Theorem 6.1.13 ([68])**.** *The maximal subgroups of* ${}^2\mathrm{F}_4(q) : f$, $f|(2m+1)$, *not containing* ${}^2\mathrm{F}_4(q)$ *are obtained from the ones in the above list by adjoining the field automorphism in the obvious way. In particular, no novelties arise.*

Lemma 6.1.14. *Let* G *be an almost simple group with socle* $G_0 = {}^2\mathrm{F}_4(q)$, *where* $q = 2^{2m+1}$ *for* $m \geq 1$. *Then*

$$P_{G,G_0}(G) \geq 1 - \frac{11}{q^{10}} - \frac{\log\log q}{q^{15}}$$

and $P_{G,G_0}(2) > 0.999$.

Proof. The order of G_0 is $q^{12}(q^6+1)(q^4-1)(q^3+1)(q-1)$. The maximal subgroups of G_0 are listed up to conjugacy in Theorem 6.1.12, and Theorem 6.1.13 tells us that G has no novelty maximal subgroups. Then let $\mathcal{L}$ be a set of conjugacy class representatives for maximal subgroups of G_0. Then we estimate the sum $\sum_{L\in\mathcal{L}} 1/[G_0 : L]$. The number of maximal subgroups of the form ${}^2\mathrm{F}_4(q_0)$ is the number of prime divisors α of $2m+1$. Then $\alpha \geq 3$ as α divides $2m+1$. Then the number of possibilities for α is bounded above by $\log\log q$, and $q_0 \leq q^{1/3}$. Then the index $[G_0 : {}^2\mathrm{F}_4(q_0)] \geq q^{15}$. There are at most 11 other maximal subgroups in $\mathcal{L}$. The subgroup with minimal index is $[q^{11}] : (\mathrm{PSL}_2(q) \times (q-1)$ which has index greater than q^{10}. Then by Lemmas 3.2.6 and Lemma 3.2.7,

$$P_{G,G_0}(2) \geq 1 - \frac{11}{q^{10}} - \frac{\log\log q}{q^{15}}.$$

This is increasing with increasing q, and as $q \geq 8$, $P_{G,G_0}(2) > 0.999$. □

When $q = 2$, the group ${}^2\mathrm{F}_4(2)$ is not simple, but the derived subgroup ${}^2\mathrm{F}_4(2)'$ is.

Lemma 6.1.15. *Let G be an almost simple group with socle $G_0 = {}^2\mathrm{F}_4(2)'$. Then $P_{G,G_0}(2) > 0.997$.*

Proof. In this case G may either be ${}^2\mathrm{F}_4(2)'$ itself, or $\mathrm{Aut}({}^2\mathrm{F}_4(2)') = {}^2\mathrm{F}_4(2)$. The exact probability for $G = {}^2\mathrm{F}_4(2)'$ has been calculated using GAP and in this case $P_{G,G_0}(2) = 1120253/1123200 > 0.997$.

When $G = {}^2\mathrm{F}_4(2)$ the maximal subgroups are given in [94] ([76] states that list in the Atlas is not complete, and gives the missing subgroup $\mathrm{SU}_3(2) : 2$). We use this information to calculate a lower bound, $P_{G,G_0}(2) > 0.998$. □

These results prove the following.

Theorem 6.1.16. *Let G be an almost simple exceptional group with socle $G_0 = {}^2\mathrm{B}_2(q)$, $\mathrm{G}_2(q)$, ${}^2\mathrm{G}_2(q)$, ${}^3\mathrm{D}_4(q)$, ${}^2\mathrm{F}_4(q)$ or ${}^2\mathrm{F}_4(2)'$. Then $P_{G,G_0}(2) > 0.931$.*

Proof. This comes from Lemmas 6.1.2, 6.1.4, 6.1.7, 6.1.9, 6.1.11, 6.1.14 and 6.1.15. □

6.2 Large rank exceptional groups

Throughout this section, unless stated otherwise, G will denote an almost simple group with socle $G_0 = \mathrm{F}_4(q)$, $\mathrm{E}_6(q)$, ${}^2\mathrm{E}_6(q)$, $\mathrm{E}_7(q)$ or $\mathrm{E}_8(q)$, where $q = p^n$ for some prime p. We divide the set of maximal subgroups M of G (where $G_0 \not\leq M$) into two subsets: the 'known' subgroups $\mathcal{K}$, and the 'unknown' subgroups $\mathcal{U}$. The subgroups $\mathcal{K}$ are those which are known up to conjugacy. Roughly speaking, the conjugacy classes of subgroups in $\mathcal{U}$ are unknown, but the subgroups are of small order and almost simple. Using the fact that all simple groups are generated by an involution and another element, together with bounds on the number of involutions in G_0, we may bound the number of subgroups in $\mathcal{U}$. Note that $\mathcal{K}$ and $\mathcal{U}$ partition the set of ordinary and novelty maximal subgroups of G, not the set of conjugacy class representatives of the maximal subgroups. Let $\mathcal{K}$ be the set of maximal subgroups M of G of the following types:

1. M is not almost simple.
2. M is almost simple such that $S = \mathrm{Soc}(M)$ is a group of Lie type over $\mathbb{F}_{p^b}$ where $\mathrm{rk}(S) > \frac{1}{2}\mathrm{rk}(G_0)$.

Let $\mathcal{U}$ be the remaining maximal subgroups M of G (where M does not contain G_0), that is, almost simple subgroups ($S = \mathrm{Soc}(M)$) of the following types:

1. S is alternating.
2. S is sporadic.
3. S is of Lie type in characteristic other than p.
4. S is of Lie type in characteristic p with $\mathrm{rk}(S) \leq \frac{1}{2}\mathrm{rk}(G_0)$.

We also assume that S is not isomorphic to a group of Lie type in characteristic p with $\mathrm{rk}(S) > \frac{1}{2}\mathrm{rk}(G_0)$.

By Lemma 3.2.6,

$$P_{G,G_0}(2) \geq 1 - \sum_{\substack{M<_{\max}G \\ G_0 \not\leq M}} \frac{1}{[G:M]^2} = 1 - \sum_{M\in\mathcal{K}} \frac{1}{[G:M]^2} - \sum_{M\in\mathcal{U}} \frac{1}{[G:M]^2},$$

and so we consider the sums over maximal subgroups in $\mathcal{K}$ and $\mathcal{U}$ in turn. Maximal subgroups of G are summarised in [59, Theorem 8], and we will look at this in more detail in the following sections.

6.2.1 Maximal subgroups of G in $\mathcal{K}$

First we determine how many conjugacy classes of subgroups M in $\mathcal{K}$ there are. We bound $[G:M]$ by the smallest degree of a non-trivial permutation representation of G_0.

Maximal subgroups of G are summarised in [59, Theorem 8]. This theorem, together with the references in [59], allow us to determine the subgroups in $\mathcal{K}$ up to conjugacy. Note that we have only stated subgroups in $\mathcal{K}$.

Theorem 6.2.1. *Let M be a maximal subgroup of G such that $M \in \mathcal{K}$. Then one of the following holds.*

1. *M is a parabolic subgroup.*
2. *M is a subgroup of maximal rank as described in [55, Tables 5.1 & 5.2].*
3. *M is the normaliser in G of an elementary abelian group E as described in [59, Theorem 8 (I)(c) & (III)].*
4. *M is almost simple and the socle of M is a subfield or twisted subgroup.*
5. *M is a maximal subgroup such that $F^*(M)$ is as described in Table 6.1.*
6. *$G_0 = \mathrm{E}_6(q)$ or ${}^2\mathrm{E}_6(q)$ and $\mathrm{Soc}(M)$ is either $C_4(q) \cong \mathrm{PSp}_8(q)$ or $\mathrm{F}_4(q)$.*
7. *$G_0 = \mathrm{E}_7(q)$ and $\mathrm{Soc}(M) = {}^3\mathrm{D}_4(q)$.*
8. *$G_0 = \mathrm{E}_8(q)$, $p > 5$ and $F^*(M) = (A_5 \times A_6)$ or $A_5 \times \mathrm{PSL}_2(q)$.*

G_0	$F^*(M)$	Conditions for p, q
$\mathrm{F}_4(q)$	$\mathrm{L}_2(q) \times \mathrm{G}_2(q)$	$p > 2, q > 3$
$\mathrm{E}_6(q)$,${}^2\mathrm{E}_6(q)$	$\mathrm{L}_3(q) \times \mathrm{G}_2(q)$	
	$\mathrm{U}_3(q) \times \mathrm{G}_2(q)$	$q > 2$
$\mathrm{E}_7(q)$	$\mathrm{L}_2(q) \times \mathrm{L}_2(q)$	$p > 3$
	$\mathrm{L}_2(q) \times \mathrm{G}_2(q)$	$p > 2, q > 3$
	$\mathrm{L}_2(q) \times \mathrm{F}_4(q)$	$q > 3$
	$\mathrm{G}_2(q) \times \mathrm{PSp}_6(q)$	
$\mathrm{E}_8(q)$	$\mathrm{L}_2(q) \times \mathrm{L}_3(q)$	$p > 3$
	$\mathrm{L}_2(q) \times \mathrm{U}_3(q)$	$p > 3$
	$\mathrm{G}_2(q) \times \mathrm{F}_4(q)$	
	$\mathrm{L}_2(q) \times \mathrm{G}_2(q) \times \mathrm{G}_2(q)$	$p > 2, q > 3$
	$\mathrm{L}_2(q) \times \mathrm{G}_2(q^2)$	$p > 2, q > 3$

Table 6.1: Maximal subgroups of G as described in [54, Table III]

Recall $F^*(M)$ is the generalised Fitting subgroup. We use Lemma 3.2.8 to bound the number of some types of subgroups up to conjugacy. In particular, we may determine the number of subgroups M up to conjugacy in $\mathrm{Inndiag}(G_0)$, the subgroup of $\mathrm{Aut}(G_0)$ generated by inner and diagonal automorphisms. Then the number of conjugates of M in G is at most $[\mathrm{Inndiag}(G_0) : G_0]$ times the number of conjugates of M in $\mathrm{Inndiag}(G_0)$. The orders of the diagonal automorphisms are given in Table 2.9, this gives the following values for $[\mathrm{Inndiag}(G_0) : G_0]$:

1. $[\mathrm{Inndiag}(\mathrm{F}_4(q)) : \mathrm{F}_4(q)] = 1$;
2. $[\mathrm{Inndiag}(\mathrm{E}_6(q)) : \mathrm{E}_6(q)] = (3, q-1)$;
3. $[\mathrm{Inndiag}({}^2\mathrm{E}_6(q)) : {}^2\mathrm{E}_6(q)] = (3, q+1)$;
4. $[\mathrm{Inndiag}(\mathrm{E}_7(q)) : \mathrm{E}_7(q)] = (2, q-1)$;
5. $[\mathrm{Inndiag}(\mathrm{E}_8(q)) : \mathrm{E}_8(q)] = 1$.

Next we calculate an upper bound on the number of conjugacy classes of maximal subgroups of each type in $\mathcal{K}$.

Lemma 6.2.2. *The number of conjugacy classes of parabolic maximal subgroups of G is bounded as follows.*

1. *If $G_0 = \mathrm{F}_4(q)$ there are at most 4 conjugacy classes of parabolic maximal subgroups.*
2. *If $G_0 = \mathrm{E}_6(q)$ or ${}^2\mathrm{E}_6(q)$ there are at most 6 conjugacy classes of parabolic maximal subgroups.*

3. *If $G_0 = \mathrm{E}_7(q)$ there are at most 7 conjugacy classes of parabolic maximal subgroups.*

4. *If $G_0 = \mathrm{E}_8(q)$ there are at most 8 conjugacy classes of parabolic maximal subgroups.*

Proof. Parabolic subgroups of G are described in [14, Section 8.3]. Up to conjugacy in G there is one maximal parabolic subgroup (that is, a subgroup which is maximal amongst the parabolic subgroups but not necessarily a maximal subgroup of G) corresponding to each node in the Dynkin diagram. Then, up to conjugacy, the number of conjugacy classes of maximal subgroups of G which are parabolic is bounded as described. □

Lemma 6.2.3. *The number of conjugacy classes of maximal subgroups of G of maximal rank are bounded as follows.*

1. *If $G_0 = \mathrm{F}_4(q)$ there are at most 14 conjugacy classes.*

2. *If $G_0 = \mathrm{E}_6(q)$ there are at most 9 conjugacy classes.*

3. *If $G_0 = {}^2\mathrm{E}_6(q)$ there are at most 9 conjugacy classes.*

4. *If $G_0 = \mathrm{E}_7(q)$ there are at most 13 conjugacy classes.*

5. *If $G_0 = \mathrm{E}_8(q)$ there are at most 29 conjugacy classes.*

Proof. Subgroups of maximal rank are listed up to conjugacy in G_0 in [55, Tables 5.1 & 5.2]. Then this gives an upper bound on the number up to conjugacy in G. □

Lemma 6.2.4. *Let M be a maximal subgroup of G such that M is the normaliser of an elementary abelian group E as described in part 3 of Theorem 6.2.1. Then the number of conjugacy classes of maximal subgroups of the form $M = N_G(E)$ is bounded as follows.*

1. *If $G_0 = \mathrm{F}_4(q)$ there is at most 1 conjugacy class.*

2. *If $G_0 = \mathrm{E}_6(q)$ there are at most 3 conjugacy classes.*

3. *If $G_0 = {}^2\mathrm{E}_6(q)$ there are at most 3 conjugacy classes.*

4. *If $G_0 = \mathrm{E}_7(q)$ there are at most 2 conjugacy classes.*

5. *If $G_0 = \mathrm{E}_8(q)$ there are at most 2 conjugacy classes.*

Proof. The elementary abelian subgroups E of G such that $M = N_G(E)$ is maximal, are given in [16, Table 1]. These correspond to the exotic maximal subgroups, or one of the subgroups of $\mathrm{E}_7(q)$ listed in [57, Theorem 8]. These subgroups are listed up to conjugacy in $\mathrm{Inndiag}(G_0)$, the group generated by

inner and diagonal automorphisms of G_0. When $G_0 = \mathrm{F}_4(q), {}^2\mathrm{E}_6(q)$, $\mathrm{E}_6(q)$ or $\mathrm{E}_7(q)$ there is at most one elementary abelian group up to conjugacy in $\mathrm{Inndiag}(G_0)$. Finally, when $G_0 = \mathrm{E}_8(q)$, there are at most 2 conjugacy classes of elementary abelian subgroups in $\mathrm{Inndiag}(\mathrm{G}_0)$. Then, to obtain an upper bound on the number of conjugacy classes of maximal subgroups of this form in G, we multiply by $[\mathrm{Inndiag}(G_0) : G_0]$. □

Lemma 6.2.5. *The number of conjugacy classes of maximal subgroups M of G such that the socle of M is a subfield or twisted subgroup is bounded as follows.*

1. *If $G_0 = \mathrm{F}_4(q)$ there are at most $2 \log q$ conjugacy classes.*
2. *If $G_0 = \mathrm{E}_6(q)$ there are at most $\frac{9}{2} \log q$ conjugacy classes.*
3. *If $G_0 = {}^2\mathrm{E}_6(q)$ there are at most $3 \log q$ conjugacy classes.*
4. *If $G_0 = \mathrm{E}_7(q)$ there are at most $2 \log q$ conjugacy classes.*
5. *If $G_0 = \mathrm{E}_8(q)$ there are at most $\log q$ conjugacy classes.*

Proof. If $q = p^f$, we get a subfield of $\mathbb{F}_q$ for each divisor of f. Then the number of subfields of $\mathbb{F}_q$ (and hence the number of different subfield subgroups) is bounded above by $\log q$. In the case of $\mathrm{E}_6(q)$ and $\mathrm{F}_4(q)$ we may also have twisted subgroups, that is subgroups of the form ${}^2\mathrm{E}_6(q_0)$ and ${}^2\mathrm{F}_4(q_0)$ respectively. Note that ${}^2\mathrm{F}_4(q_0) \leq \mathrm{F}_4(q_0)$, but ${}^2\mathrm{E}_6(q_0)$ is not embedded in $\mathrm{E}_6(q_0)$ but in $\mathrm{E}_6(q_0^2)$. The number of twisted subgroups of the form ${}^2\mathrm{F}_4(q_0)$ is bounded above by the number of subfields, which itself is bounded by $\log q$. The number of subgroups of $\mathrm{E}_6(q)$ of the form ${}^2\mathrm{E}_6(q)$ is bounded above by $\log q^{\frac{1}{2}} = (\log q)/2$. By [59, Theorem 8], these classes are given up to conjugacy in $\mathrm{Inndiag}(G_0)$, and so we multiply by $[\mathrm{Inndiag}(G_0) : G_0]$ to obtain an upper bound for the number of conjugacy classes of maximal subgroups of this form in G. □

Lemma 6.2.6. *The number of conjugacy classes of maximal subgroups $M \in \mathcal{K}$ of G is bounded as follows.*

1. *If $G_0 = \mathrm{F}_4(q)$ the number of conjugacy classes of subgroups in $\mathcal{K}$ is at most $20 + 2 \log q$.*
2. *If $G_0 = \mathrm{E}_6(q)$ the number of conjugacy classes of subgroups in $\mathcal{K}$ is at most $30 + \frac{9}{2} \log q$.*
3. *If $G_0 = {}^2\mathrm{E}_6(q)$ the number of conjugacy classes of subgroups in $\mathcal{K}$ is at most $30 + 3 \log q$.*
4. *If $G_0 = \mathrm{E}_7(q)$ the number of conjugacy classes of subgroups in $\mathcal{K}$ is at most $32 + 2 \log q$.*

5. *If* $G_0 = \mathrm{E}_8(q)$ *the number of conjugacy classes of subgroups in* $\mathcal{K}$ *is at most* $46 + \log q$.

Proof. We use Theorem 6.2.1 and consider each case separately. The number of conjugacy classes of maximal subgroups which are parabolic, of maximal rank, normalisers of elementary abelian subgroups, or subfield or twisted subgroups, are given in Lemmas 6.2.2, 6.2.3, 6.2.4 and 6.2.5.

The remaining subgroups are either those listed in Table 6.1, or subgroups of $\mathrm{E}_6(q)$, ${}^2\mathrm{E}_6(q)$, $\mathrm{E}_7(q)$ or $\mathrm{E}_8(q)$ given in parts 6, 7, 8 of Theorem 6.2.1. These are given up to conjugacy in $\mathrm{Inndiag}(G_0)$ and so we multiply the number of subgroups by $[\mathrm{Inndiag}(G_0) : G_0]$ to get an upper bound on the number of conjugacy classes in G. □

By Lemma 3.2.7, the index of a maximal subgroup in G, $[G : M]$, is bounded below by the minimal degree of a non-trivial permutation representation of G_0. These degrees are given in [88], [89], [90] and we summarize them in the following theorem.

Theorem 6.2.7. *Let* G_0 *be an finite simple exceptional group. Then the minimal degree,* $\rho(G_0)$*, of a faithful permutation representation of* G_0 *is as follows.*

1. *If* $G_0 = \mathrm{F}_4(q)$*, then*

$$\rho(G_0) = \frac{(q^{12}-1)(q^4+1)}{(q-1)}.$$

2. *If* $G_0 = \mathrm{E}_6(q)$*, then*

$$\rho(G_0) = \frac{(q^9-1)(q^8+q^4+1)}{(q-1)}.$$

3. *If* $G_0 = {}^2\mathrm{E}_6(q)$*, then*

$$\rho(G_0) = \frac{(q^{12}-1)(q^6-q^3+1)(q^4+1)}{(q-1)}.$$

4. *If* $G_0 = \mathrm{E}_7(q)$*, then*

$$\rho(G_0) = \frac{(q^{14}-1)(q^9+1)(q^5+1)}{(q-1)}.$$

5. *If* $G_0 = \mathrm{E}_8(q)$*, then*

$$\rho(G_0) = \frac{(q^{30}-1)(q^{12}+1)(q^{10}+1)(q^6+1)}{(q-1)}.$$

Then we obtain an estimate for

$$\sum_{M\in\mathcal{K}} \frac{1}{[G:M]^2}.$$

Lemma 6.2.8. *We may bound* $\sum_{M\in\mathcal{K}} 1/[G:M]^2$ *as follows.*

1. *Let* $G_0 = \mathrm{F}_4(q)$. *Then*

$$\sum_{M\in\mathcal{K}} \frac{1}{[G:M]^2} \leq \frac{(20+2\log q)(q-1)}{(q^{12}-1)(q^4+1)}.$$

2. *Let* $G_0 = \mathrm{E}_6(q)$. *Then*

$$\sum_{M\in\mathcal{K}} \frac{1}{[G:M]^2} \leq \frac{(60+9\log q)(q-1)}{2(q^9-1)(q^8+q^4+1)}.$$

3. *Let* $G_0 = {}^2\mathrm{E}_6(q)$. *Then*

$$\sum_{M\in\mathcal{K}} \frac{1}{[G:M]^2} \leq \frac{(30+3\log q)(q-1)}{(q^{12}-1)(q^6-q^3+1)(q^4+1)}.$$

4. *Let* $G_0 = \mathrm{E}_7(q)$. *Then*

$$\sum_{M\in\mathcal{K}} \frac{1}{[G:M]^2} \leq \frac{(32+2\log q)(q-1)}{(q^{14}-1)(q^9+1)(q^5+1)}.$$

5. *Let* $G_0 = \mathrm{E}_8(q)$. *Then*

$$\sum_{M\in\mathcal{K}} \frac{1}{[G:M]^2} \leq \frac{(46+\log q)(q-1)}{(q^{30}-1)(q^{12}+1)(q^{10}+1)(q^6+1)}.$$

Proof. Let $\mathcal{M}_K$ be a set of conjugacy class representatives for maximal subgroups $M \in \mathcal{K}$. Then $\sum_{M\in\mathcal{K}} 1/[G:M]^2 \leq \sum_{M\in\mathcal{M}_K} 1/[G:M]$ as the number of conjugates of M, $[G : N_G(M)]$, is bounded above by $[G : M]$. By Lemma 3.2.7, $[G : M]$ may be bounded below by the smallest degree of a permutation representation of G_0. We bound this using Theorem 6.2.7. Lemma 6.2.6 gives an upper bound for the number of maximal subgroups in $\mathcal{M}_K$. The result follows. □

6.2.2 Maximal subgroups of G in $\mathcal{U}$

Now consider subgroups $M \in \mathcal{U}$, where $\mathrm{Soc}(M) = S$ for some simple group S which is alternating, sporadic, of Lie type in cross-characteristic, or of Lie type in defining characterisitic with $\mathrm{rk}(S) \leq \frac{1}{2}\mathrm{rk}(G_0)$. In fact, $M = N_G(S)$ and so for each simple group $S < G$ (of the appropriate type), we have at most one maximal subgroup $M \in \mathcal{U}$ such that $\mathrm{Soc}(M) = S$. So we may obtain an upper bound on the number of subgroups in $\mathcal{U}$ by estimating the number of simple groups that may be socles of subgroups in $\mathcal{U}$. Note that in this case we are estimating the actual number of subgroups in $\mathcal{U}$, and not the number up to conjugacy.

Let $\mathcal{U}_s$ denote the set of socles of $M \in \mathcal{U}$. For $M \in \mathcal{U}$, $G_0 \cap M \trianglelefteq M$ is also an almost simple subgroup of G_0 with socle S. Then the number of subgroups in $\mathcal{U}$ may be bounded above by the number of simple subgroups in G_0. As we shall see, this is bounded using the fact that every simple group can be generated by an involution and another element, and we have a bound on the number of involutions in G_0. We may determine all the possibilities for $S \in \mathcal{U}_s$ and therefore we obtain an upper bound on $|M| \leq |\mathrm{Aut}(S)|$. This gives us a lower bound, $[G : M] \geq |G_0|/|\mathrm{Aut}(S)|$.

Theorem 6.2.9 ([62, Theorem 1.2])**.** *Let M be a maximal subgroup of G where $S = \mathrm{Soc}(M)$ is a group of Lie type in defining characteristic such that such that $\mathrm{rk}(S) \leq \frac{1}{2}\mathrm{rk}(G_0)$. Then*

1. *if $G_0 = \mathrm{F}_4(q)$ then $|M| < 4q^{20}\log_p q$;*
2. *if $G_0 = \mathrm{E}_6(q)$ or ${}^2\mathrm{E}_6(q)$ then $|M| < 4q^{28}\log_p q$;*
3. *if $G_0 = \mathrm{E}_7(q)$ then $|M| < 4q^{30}\log_p q$;*
4. *if $G_0 = \mathrm{E}_8(q)$ then $|M| < 12q^{56}\log_p q$.*

This only deals with subgroups in $\mathcal{U}$ in defining characteristic. In fact, there are further restrictions on the socles of subgroups in $\mathcal{U}$ given in [59, Theorem 8]. We will use these in the following section when we consider $G_0 = \mathrm{F}_4(q)$ for $q \leq 16$, $\mathrm{E}_6(3)$ and ${}^2\mathrm{E}_6(3)$, but for the general case the bound above suffices. The remaining subgroups M are almost simple groups with socle S, where S is sporadic, alternating or of Lie type in cross-characteristic. All possibilities for simple groups $S < G_0$ where S is alternating, sporadic or of Lie type in different characteristic to G_0 are listed in [60, Theorem 1] which gives the following.

Theorem 6.2.10. *Let S be a simple subgroup of G, where S is alternating, sporadic, or of Lie type in cross-characteristic. Then we have the following possibilities.*

1. *If $G_0 = \mathrm{F}_4(q)$ then S is one of the groups in Table 6.2.*

S	$\lvert S\rvert$	$\lvert\mathrm{Out}(S)\rvert$
$A_5 \cong \mathrm{PSL}_2(4) \cong \mathrm{PSL}_2(5)$	$2^2.3.5$	2
$A_6 \cong \mathrm{PSL}_2(9)$	$2^3.3^2.5$	4
A_7	$2^3.3^2.5.7$	2
$A_8 \cong \mathrm{PSL}_4(2)$	$2^6.3^2.5.7$	2
A_9	$2^6.3^4.5.7$	2
A_{10}	$2^7.3^4.5^2.7$	2
A_{11} $(p = 11)$	$2^7.3^4.5^2.7.11$	2
$\mathrm{PSL}_2(7) \cong \mathrm{PSL}_3(2)$	$2^3.3.7$	2
$\mathrm{PSL}_2(8)$	$2^3.3^2.7$	3
$\mathrm{PSL}_2(13)$	$2^2.3.7.13$	2
$\mathrm{PSL}_2(17)$	$2^4.3^2.17$	2
$\mathrm{PSL}_2(25)$	$2^3.3.5^2.13$	4
$\mathrm{PSL}_2(27)$	$2^2.3^3.7.13$	6
$\mathrm{PSL}_3(3)$	$2^4.3^3.13$	2
$\mathrm{PSL}_3(4)$ $(p = 3)$	$2^6.3^2.5.7$	12
$\mathrm{PSL}_4(3)$ $(p = 2)$	$2^7.3^6.5.13$	4
$\mathrm{PSU}_3(3)$	$2^5.3^3.7$	2
$\mathrm{PSU}_4(2) \cong \mathrm{PSp}_4(3)$	$2^6.3^4.5$	2
$\mathrm{PSp}_6(2)$	$2^9.3^4.5.7$	1
$\mathrm{P}\Omega_8^+(2)$	$2^{12}.3^5.5^2.7$	6
${}^3\mathrm{D}_4(2)$	$2^{12}.3^4.7^2.13$	3
${}^2\mathrm{B}_2(8)$ $(p = 5)$	$2^6.5.7.13$	3
M_{11} $(p = 11)$	$2^4.3^2.5.11$	1
J_1 $(p = 11)$	$2^3.3.5.7.11.19$	1
J_2	$2^7.3^3.5^2.7$	2

Table 6.2: Possible simple subgroups of $\mathrm{F}_4(q)$, $\mathrm{E}_6(q)$, ${}^2\mathrm{E}_6(q)$, $\mathrm{E}_7(q)$ and $\mathrm{E}_8(q)$

2. *If $G_0 = \mathrm{E}_6(q)$ or ${}^2\mathrm{E}_6(q)$ then S is one of the groups in Table 6.2 or Table 6.3.*

3. *If $G_0 = \mathrm{E}_7(q)$ then S is one of the groups in Table 6.2, Table 6.3 or Table 6.4.*

4. *If $G_0 = \mathrm{E}_8(q)$ then S is one of the groups in Table 6.2, Table 6.3, Table 6.4, or Table 6.5.*

We wish to find an upper bound for the order of maximal subgroups $M \in \mathcal{U}$. We already have a bound when the socle S is of Lie type in defining characteristic, we seek a bound for the cases where the S is sporadic, alternating or of Lie type in cross-characteristic. We use Theorem 6.2.10 to determine possibilities for S. Full maximal subgroup information is available for almost simple groups with socles $\mathrm{F}_4(2)$, $\mathrm{E}_6(2)$ or ${}^2\mathrm{E}_6(2)$. So it suffices to

S	$\lvert S\rvert$	$\lvert\mathrm{Out}(S)\rvert$
A_{11}	$2^7.3^4.5^2.7.11$	2
A_{12} $(p=2,3)$	$2^9.3^5.5^2.7.11$	2
$\mathrm{PSL}_2(11)$	$2^2.3.5.11$	2
$\mathrm{PSL}_2(19)$	$2^2.3^2.5.19$	2
$\mathrm{PSL}_3(4)$	$2^6.3^2.5.7$	12
$\mathrm{PSU}_4(3)$	$2^7.3^6.5.7$	8
$\Omega_7(3)$ $(p=2)$	$2^9.3^9.5.7.13$	2
$\mathrm{G}_2(3)$ $(p=2)$	$2^6.3^6.7.13$	2
${}^2\mathrm{F}_4(2)'$	$2^{11}.3^3.5^2.13$	2
M_{11}	$2^4.3^2.5.11$	1
M_{12} $(p=2,3,5)$	$2^6.3^3.5.11$	2
M_{22} $(p=2,7)$	$2^7.3^2.5.7.11$	2
J_3 $(p=2)$	$2^7.3^5.5.17.19$	2
Fi_{22} $(p=2)$	$2^{17}.3^9.5^2.7.11.13$	2

Table 6.3: Possible simple subgroups of $\mathrm{E}_6(q)$, ${}^2\mathrm{E}_6(q)$, $\mathrm{E}_7(q)$ and $\mathrm{E}_8(q)$

S	$\lvert S\rvert$	$\lvert\mathrm{Out}(S)\rvert$
A_{12}	$2^9.3^5.5^2.7.11$	2
A_{13}	$2^9.3^5.5^2.7.11.13$	2
A_{14} $(p=7)$	$2^{10}.3^5.5^2.7^2.11.13$	2
$\mathrm{PSL}_2(29)$	$2^2.3.5.7.29$	2
$\mathrm{PSL}_2(37)$	$2^2.3^2.19.37$	2
$\mathrm{PSU}_3(8)$	$2^9.3^4.7.19$	18
M_{12}	$2^6.3^3.5.11$	2
M_{22} $(p=5)$	$2^7.3^2.5.7.11$	2
Ru $(p=5)$	$2^{14}.3^3.5^3.7.13.29$	1
HS $(p=5)$	$2^9.3^2.5^3.7.11$	2

Table 6.4: Possible simple subgroups of $\mathrm{E}_7(q)$ and $\mathrm{E}_8(q)$

S	$\lvert S\rvert$	$\lvert\mathrm{Out}(S)\rvert$
A_{14}	$2^{10}.3^5.5^2.7^2.11.13$	2
A_{15}	$2^{10}.3^6.5^3.7^2.11.13$	2
A_{16}	$2^{14}.3^6.5^3.7^2.11.13$	2
A_{17}	$2^{14}.3^6.5^3.7^2.11.13.17$	2
A_{18} $(p=3)$	$2^{15}.3^8.5^3.7^2.11.13.17$	2
$\mathrm{PSL}_2(16)$	$2^4.3.5.17$	4
$\mathrm{PSL}_2(31)$	$2^5.3.5.31$	2
$\mathrm{PSL}_2(32)$	$2^5.3.11.31$	5
$\mathrm{PSL}_2(41)$	$2^3.3.5.7.41$	2
$\mathrm{PSL}_2(49)$	$2^4.3.5^2.7^2$	4
$\mathrm{PSL}_2(61)$	$2^2.3.5.31.61$	2
$\mathrm{PSL}_3(5)$	$2^5.3.5^3.31$	2
$\mathrm{PSL}_4(5)$ $(p=2)$	$2^7.3^2.5^6.13.31$	8
$\mathrm{PSp}_4(5)$	$2^6.3^2.5^4.13$	2
$\mathrm{G}_2(3)$	$2^6.3^6.7.13$	2
${}^2\mathrm{B}_2(8)$	$2^6.5.7.13$	3
${}^2\mathrm{B}_2(32)$ $(p=5)$	$2^{10}.5^2.31.41$	5
Th $(p=3)$	$2^{15}.3^{10}.5^3.7^2.13.19.31$	1

Table 6.5: Possible simple subgroups of $\mathrm{E}_8(q)$

calculate upper bounds on the order of maximal subgroups $M \in \mathcal{U}$ in the cases where G_0 is one of $\mathrm{F}_4(q)$, $\mathrm{E}_6(q)$ and ${}^2\mathrm{E}_6(q)$ when $q \geq 3$. We consider $\mathrm{F}_4(3)$, $\mathrm{F}_4(4)$, $\mathrm{F}_4(8)$, $\mathrm{F}_4(9)$, $\mathrm{F}_4(16)$, ${}^2\mathrm{E}_6(3)$ and $\mathrm{E}_6(3)$ in more detail later as we have to be more careful with the estimates for these groups.

Lemma 6.2.11. *Let S be a simple subgroup of $\mathrm{F}_4(q)$ where $q \geq 3$ and S is alternating, sporadic, or of Lie type in cross-characteristic. Then $|\mathrm{Aut}(S)| \leq 4q^{20}\log q$.*

Proof. The possibilities for S come from Theorem 6.2.10. In all cases $|\mathrm{Aut}(S)|$ is at most $|\mathrm{Aut}(\mathrm{P}\Omega_8^+(2))| \leq 4q^{20}\log q$. □

Lemma 6.2.12. *Let S be a simple subgroup of $\mathrm{E}_6(q)$ or ${}^2\mathrm{E}_6(q)$ where $q \geq 3$ and S is alternating, sporadic, or of Lie type in cross-characteristic. Then $|\mathrm{Aut}(S)| \leq 4q^{28}\log q$.*

Proof. The possibilities for S come from Theorem 6.2.10. We see that $|\mathrm{Aut}(S)|$ is largest when $S = \mathrm{Fi}_{22}$. This subgroup only occurs when $p = 2$, and for $q \geq 4$, $|\mathrm{Aut}(S)| \leq |\mathrm{Aut}(\mathrm{Fi}_{22})| \leq 4q^{28}\log q$. If $q = 3$ then $|\mathrm{Aut}(S)| \leq 4.3^{28}\log 3$. So the bound holds for all $q \geq 3$. □

Lemma 6.2.13. *Let S be a simple subgroup $\mathrm{E}_7(q)$ where S is alternating, sporadic, or of Lie type in cross-characteristic. Then $|\mathrm{Aut}(S)| \leq 9q^{30}\log q$.*

Proof. The possibilities for S come from Theorem 6.2.10. By [46], Fi_{22} is not a subgroup of $\mathrm{E}_7(q)$. If $q \geq 5$, then $|\mathrm{Aut}(S)| \leq |\mathrm{Aut}(\mathrm{Ru})| \leq 9.5^{30}(\log 5)$. Otherwise, if $q \leq 4$, then $|\mathrm{Aut}(S)| \leq |\mathrm{Aut}(\Omega_7(3))| \leq 9.2^{30}$ as required. □

Lemma 6.2.14. *Let S be a simple subgroup of $\mathrm{E}_8(q)$ where S is alternating, sporadic, or of Lie type in cross-characteristic. Then $|\mathrm{Aut}(S)| \leq 12q^{56}\log q$.*

Proof. By Theorem 6.2.10, $|\mathrm{Aut}(S)| \leq |\mathrm{Aut}(\mathrm{Th})| \leq 12q^{56}\log q$. □

Lemma 6.2.15. *Let M be a maximal subgroup of G lying in $\mathcal{U}$. The order of M is bounded as follows.*

1. *If $G_0 = \mathrm{F}_4(q)$ then $|M| < 4q^{20}\log q$ for $q \geq 3$.*
2. *If $G_0 = \mathrm{E}_6(q)$ or ${}^2\mathrm{E}_6(q)$ then $|M| < 4q^{28}\log q$ for $q \geq 3$.*
3. *If $G_0 = \mathrm{E}_7(q)$ then $|M| < 9q^{30}\log q$.*
4. *If $G_0 = \mathrm{E}_8(q)$ then $|M| < 12q^{56}\log q$.*

Proof. Let $S = \mathrm{Soc}(M)$. Theorem 6.2.9 above shows that these bounds hold when S is a group of Lie type in the same characteristic as G_0, and where $\mathrm{rk}(S) \leq \frac{1}{2}\mathrm{rk}(G_0)$. Otherwise S is alternating, sporadic or of Lie type in a different characteristic to G. In these cases the bounds hold by Lemmas 6.2.11 – 6.2.14. □

We use Lemma 3.2.12 to estimate the number of maximal subgroups of G in $\mathcal{U}$ and so we wish to estimate the number of involutions for each possible G_0. The conjugacy classes of involutions of $G_0 = \mathrm{F}_4(q)$, ${}^2\mathrm{E}_6(q)$, $\mathrm{E}_6(q)$, $\mathrm{E}_7(q)$ and $\mathrm{E}_8(q)$ have been determined in [3] and [37]. As described in [62] in all cases there are at most 5 classes of involutions and the centralisers of involutions in conjugacy classes of maximal size are as in Table 6.6 (from [62, Table II]). Then $i(G_0) \leq 5[G_0 : C_{G_0}(t)]$ where t is an involution in a

G_0	$\lvert C_{G_0}(t)\rvert$, q even	$\lvert C_{G_0}(t)\rvert$, q odd
$\mathrm{F}_4(q)$	$q^{18}\lvert\mathrm{SL}_2(q)\rvert^2$	$\lvert\mathrm{SL}_2(q)\rvert\lvert\mathrm{Sp}_6(q)\rvert$
$\mathrm{E}_6(q)$	$q^{27}\lvert\mathrm{SL}_2(q)\rvert\lvert\mathrm{PSL}_3(q)\rvert$	$1/(3,q-1)\lvert\mathrm{SL}_2(q)\rvert\lvert\mathrm{SL}_6(q)\rvert$
${}^2\mathrm{E}_6(q)$	$q^{27}\lvert\mathrm{SU}_2(q)\rvert\lvert\mathrm{PSU}_3(q)\rvert$	$1/(3,q+1)\lvert\mathrm{SL}_2(q)\rvert\lvert\mathrm{SU}_6(q)\rvert$
$\mathrm{E}_7(q)$	$q^{42}\lvert\mathrm{Sp}_6(q)\rvert$	$\frac{1}{2}\lvert\mathrm{SL}_8(q)\rvert$ if $q = 1 \mod 4$
		$\frac{1}{2}\lvert\mathrm{SU}_8(q)\rvert$ if $q = -1 \mod 4$
$\mathrm{E}_8(q)$	$q^{84}\lvert\mathrm{Sp}_8(q)\rvert$	$4\lvert\mathrm{P}\Omega^+_{16}(q)\rvert$

Table 6.6: Centralisers of involutions in conjugacy classes of maximal size

conjugacy class of maximal size.

Lemma 6.2.16. *Let $G_0 = \mathrm{F}_4(q)$ for $q \geq 3$. Then*

$$\sum_{M \in \mathcal{U}} \frac{1}{[G:M]^2} \leq \frac{2640q^{10}(\log q)^2}{7(q^2-1)^2(q^4-1)(q^6-1)}.$$

Proof. By Lemma 3.2.12,

$$\sum_{M \in \mathcal{U}} \frac{1}{[G:M]^2} \leq \frac{6i(G_0)m \log m}{7|G_0|}$$

where m is an upper bound for maximal subgroups in $\mathcal{U}$. We may take $m = 4q^{20} \log q$ by Lemma 6.2.15. There are at most 5 conjugacy classes of involutions and so we bound $i(G_0)$ by $5[G_0 : C_{G_0}(t)]$ where t is an involution in a conjugacy class of maximal size. Table 6.6 gives the order of $|C_{G_0}(t)|$. If q is even,

$$|C_{G_0}(t)| = q^{18}|\mathrm{SL}_2(q)|^2 = q^{20}(q^2-1)^2$$

and if q is odd,

$$|C_{G_0}(t)| = |\mathrm{SL}_2(q)||\mathrm{Sp}_6(q)| = q^{10}(q^2-1)^2(q^4-1)(q^6-1).$$

In both cases

$$|C_{G_0}(t)| \geq q^{10}(q^2-1)^2(q^4-1)(q^6-1).$$

Then

$$\begin{aligned}
\sum_{M \in \mathcal{U}} \frac{1}{[G:M]^2} &\leq \frac{30m \log m}{7|C_{G_0}(t)|} \\
&\leq \frac{(120q^{20} \log q)(2 + \log\log q + 20 \log q)}{7q^{10}(q^2-1)^2(q^4-1)(q^6-1)} \\
&\leq \frac{(120q^{20} \log q)(22 \log q)}{7q^{10}(q^2-1)^2(q^4-1)(q^6-1)} \\
&\leq \frac{2640q^{10}(\log q)^2}{7(q^2-1)^2(q^4-1)(q^6-1)}.
\end{aligned}$$

□

Lemma 6.2.17. *Let $G_0 = \mathrm{E}_6(q)$ for $q \geq 3$. Then*

$$\sum_{M \in \mathcal{U}} \frac{1}{[G:M]} \leq \frac{10800q^{12}(\log q)^2}{7(q^2-1)\prod_{i=2}^{6}(q^i-1)}.$$

Proof. By Lemma 3.2.12,

$$\sum_{M \in \mathcal{U}} \frac{1}{[G:M]} \leq \frac{6i(G_0)m \log m}{7|G_0|}$$

where m is an upper bound for maximal subgroups in $\mathcal{U}$. We take $m = 4q^{28}\log q$ from Lemma 6.2.15. Let t be an involution in a conjugacy class of maximal size. By Table 6.6 if q is even,

$$|C_{G_0}(t)| = q^{27}|\mathrm{SL}_2(q)||\mathrm{PSL}_3(q)| \geq q^{31}(q^2-1)^2(q^3-1).$$

If q is odd,

$$|C_{G_0}(t)| = \frac{1}{(3,q-1)}|\mathrm{SL}_2(q)||\mathrm{SL}_6(q)| \geq \frac{1}{3}q^{16}(q^2-1)\prod_{i=2}^{6}(q^i-1).$$

Then in both cases

$$|C_{G_0}(t)| \geq \frac{1}{3}q^{16}(q^2-1)\prod_{i=2}^{6}(q^i-1).$$

There are at most 5 conjugacy classes of involutions and so $i(G_0) \leq 5[G_0 : C_{G_0}(t)]$. Then

$$\begin{aligned}
\sum_{M\in\mathcal{U}}\frac{1}{[G:M]^2} &\leq \frac{30m\log m}{7|C_{G_0}(t)|}\\
&\leq \frac{360q^{28}\log q\log(4q^{28}\log q)}{7q^{16}(q^2-1)\prod_{i=2}^{6}(q^i-1)}\\
&\leq \frac{(360q^{28}\log q)(2+28\log q+\log\log q)}{7q^{16}(q^2-1)\prod_{i=2}^{6}(q^i-1)}\\
&\leq \frac{(360q^{28}\log q)(30\log q)}{7q^{16}(q^2-1)\prod_{i=2}^{6}(q^i-1)}\\
&\leq \frac{10800q^{12}(\log q)^2}{7(q^2-1)\prod_{i=2}^{6}(q^i-1)}.
\end{aligned}$$

□

Lemma 6.2.18. *Let $G_0 = {}^2\mathrm{E}_6(q)$ for $q \geq 3$. Then*

$$\sum_{M\in\mathcal{U}}\frac{1}{[G:M]} \leq \frac{10800q^{12}(\log q)^2}{7(q^2-1)\prod_{i=2}^{6}(q^i-(-1)^i)}.$$

Proof. By Lemma 3.2.12,

$$\sum_{M\in\mathcal{U}}\frac{1}{[G:M]^2} \leq \frac{6i(G_0)m\log m}{7|G_0|}$$

where we may take $m = 4q^{28}\log q$ by Lemma 6.2.15. Table 6.6 gives the order of $|C_{G_0}(t)|$ where t is an involution in a conjugacy class of maximal

size. We estimate the number of involutions using $i(G_0) \leq 5[G_0 : C_{G_0}(t)]$. If q is even

$$|C_{G_0}(t)| = q^{27}|\mathrm{SU}_2(q)||\mathrm{PSU}_3(q)| = \frac{1}{(3, q+1)}q^{31}(q^2-1)^2(q^3+1).$$

If q is odd

$$|C_{G_0}(t)| = \frac{1}{(3, q+1)}q^{16}(q^2-1)^2(q^3+1)(q^4-1)(q^5+1)(q^6-1).$$

Then for all q,

$$|C_{G_0}(t)| \geq \frac{1}{3}q^{16}(q^2-1)^2(q^3+1)(q^4-1)(q^5+1)(q^6-1).$$

As $\log m \leq 30 \log q$ we bound the sum as follows,

$$\begin{aligned}\sum_{M \in \mathcal{U}} \frac{1}{[G:M]^2} &\leq \frac{30m \log m}{7|C_{G_0}(t)|} \\ &\leq \frac{10800q^{12}(\log q)^2}{7(q^2-1)\prod_{i=2}^{6}(q^i-(-1)^i)}.\end{aligned}$$

□

Lemma 6.2.19. *Let $G_0 = \mathrm{E}_7(q)$. Then*

$$\sum_{M \in \mathcal{U}} \frac{1}{[G:M]^2} \leq \frac{18360q^2(\log q)^2}{7\prod_{i=2}^{8}(q^i-1)}.$$

Proof. By Lemma 3.2.12,

$$\sum_{M \in \mathcal{U}} \frac{1}{[G:M]} \leq \frac{6i(G_0)m \log m}{7|G_0|},$$

where we may take $m = 9q^{30} \log q$ by Lemma 6.2.15. Let t be an involution in a conjugacy class of maximal size. By Table 6.6 if q is odd,

$$|C_{G_0}(t)| = q^{42}|\mathrm{Sp}_6(q)| = q^{51}(q^2-1)(q^4-1)(q^6-1).$$

If q is even $|C_{G_0}(t)| = \frac{1}{2}|\mathrm{SL}_8(q)|$ or $\frac{1}{2}|\mathrm{SU}_8(q)|$ and so

$$|C_{G_0}(t)| \geq \frac{1}{2}q^{28}\prod_{i=2}^{8}(q^i-1).$$

In all cases,

$$|C_{G_0}(t)| \geq \frac{1}{2}q^{28}\prod_{i=2}^{8}(q^i-1).$$

There are at most 5 conjugacy classes of involutions in G_0 and therefore $i(G_0) \leq 5[G_0 : C_{G_0}(t)]$. Then

$$\begin{aligned}
\sum_{M \in \mathcal{U}} \frac{1}{[G:M]^2} &\leq \frac{6i(G_0)m\log m}{7|G|} \\
&\leq \frac{30m\log m}{7|C_{G_0}(t)|} \\
&\leq \frac{60m\log m}{7q^{28}\prod_{i=2}^{8}(q^i-1)} \\
&\leq \frac{(540q^{30}\log q)\log(9q^{30}\log q)}{7q^{28}\prod_{i=2}^{8}(q^i-1)} \\
&\leq \frac{(540q^{30}\log q)(34\log q)}{7q^{28}\prod_{i=2}^{8}(q^i-1)} \\
&\leq \frac{18360q^2(\log q)^2}{7\prod_{i=2}^{8}(q^i-1)}.
\end{aligned}$$

□

Lemma 6.2.20. *Let $G_0 = \mathrm{E}_8(q)$. Then*

$$\sum_{M \in \mathcal{U}} \frac{1}{[G:M]^2} \leq \frac{21600(\log q)^2}{7(q^8-1)\prod_{i=1}^{7}(q^{2i}-1)}.$$

Proof. By Lemma 3.2.12

$$\sum_{M \in \mathcal{U}} \frac{1}{[G:M]^2} \leq \frac{6i(G_0)m\log m}{7|G_0|}$$

where m is an upper bound on the order of maximal subgroups in $\mathcal{U}$. By Lemma 6.2.15, we may take $m = 12q^{56}\log q$. Let t be an involution in a conjugacy class of maximal size. Then the conjugacy class has order $[G_0 : C_{G_0}(t)]$ and there are at most 5 conjugacy classes of involutions in G. The number of involutions in G is bounded above by $i(G_0) \leq 5[G_0 : C_{G_0}(t)]$ and so

$$\sum_{M \in \mathcal{U}} \frac{1}{[G:M]^2} \leq \frac{30m\log m}{7|C_{G_0}(t)|}.$$

Table 6.6 gives the order of $|C_{G_0}(t)|$. If q is even,

$$|C_{G_0}(t)| = q^{84}|\mathrm{Sp}_8(q)| = q^{100}(q^2-1)(q^4-1)(q^6-1)(q^8-1),$$

and if q is odd,

$$|C_{G_0}(t)| = 4|\mathrm{P}\Omega_{16}^{+}(q)| \geq q^{56}(q^8-1)\prod_{i=1}^{7}(q^{2i}-1).$$

In both cases

$$|C_{G_0}(t)| \geq q^{56}(q^8-1)\prod_{i=1}^{7}(q^{2i}-1)$$

and so

$$\begin{aligned}\sum_{M\in\mathcal{U}}\frac{1}{[G:M]^2} &\leq \frac{30m\log m}{7q^{56}(q^8-1)\prod_{i=1}^{7}(q^{2i}-1)}\\ &\leq \frac{30(12q^{56}\log q)\log(12q^{56}\log q)}{7q^{56}(q^8-1)\prod_{i=1}^{7}(q^{2i}-1)}\\ &\leq \frac{30(12q^{56}\log q)(60\log q)}{7q^{56}(q^8-1)\prod_{i=1}^{7}(q^{2i}-1)}\\ &\leq \frac{21600(\log q)^2}{7(q^8-1)\prod_{i=1}^{7}(q^{2i}-1)}.\end{aligned}$$

□

6.3 Estimates for $P_{G,G_0}(2)$ for large rank exceptional groups

We now combine the results from the previous section. We have estimates for $\sum_{M\in\mathcal{K}}1/[G:M]^2$ and $\sum_{M\in\mathcal{U}}1/[G:M]^2$ from Theorem 6.2.8 and Lemmas 6.2.16 – 6.2.20. From this we estimate

$$P_{G,G_0}(2) \geq 1-\left(\sum_{M\in\mathcal{K}}\frac{1}{[G:M]^2}+\sum_{M\in\mathcal{U}}\frac{1}{[G:M]^2}\right)$$

and bounds for specific groups are given below. In each case the bounds are increasing with increasing q, and so we may obtain lower bounds for the probability. For $G_0=\mathrm{F}_4(q)$ with $q\leq 17$, and $G_0=\mathrm{E}_6(q)$ or ${}^2\mathrm{E}_6(q)$ with $q=2,3$, these probability estimates are not good enough to show $P_{G,G_0}(2)>0.931$ (although in the cases $G_0=\mathrm{F}_4(16)$, $\mathrm{F}_4(17)$, $\mathrm{E}_6(3)$ and ${}^2\mathrm{E}_6(3)$ these estimates are good enough to show $P_{G,G_0}(2)>0.9$). We consider better estimates for these small groups in the following section.

Theorem 6.3.1. *Let $G_0=\mathrm{F}_4(q)$ for $q\geq 3$. Then*

$$P_{G,G_0}(2)\geq 1-\frac{(20+2\log q)(q-1)}{(q^{12}-1)(q^4+1)}-\frac{2640q^{10}(\log q)^2}{7(q^2-1)^2(q^4-1)(q^6-1)}$$

and if $q\geq 19$ then $P_{G,G_0}(2)>0.947$.

Theorem 6.3.2. *Let $G_0=\mathrm{E}_6(q)$ for $q\geq 3$. Then*

$$P_{G,G_0}(2)\geq 1-\frac{(60+9\log q)(q-1)}{2(q^9-1)(q^8+q^4+1)}-\frac{10800q^{12}(\log q)^2}{7(q^2-1)\prod_{i=2}^{6}(q^i-1)}$$

and if $q\geq 4$ then $P_{G,G_0}(2)>0.993$.

Theorem 6.3.3. *Let $G_0 = {}^2\mathrm{E}_6(q)$ for $q \geq 3$. Then*

$$P_{G,G_0}(2) \geq 1 - \frac{(30 + 3\log q)(q-1)}{(q^{12}-1)(q^6-q^3+1)(q^4+1)} - \frac{10800q^{12}(\log q)^2}{7(q^2-1)\prod_{i=2}^{6}(q^i-(-1)^i)}$$

and if $q \geq 4$ then $P_{G,G_0}(2) > 0.993$.

Theorem 6.3.4. *Let $G_0 = \mathrm{E}_7(q)$. Then*

$$P_{G,G_0}(2) \geq 1 - \frac{(32 + 2\log q)(q-1)}{(q^{14}-1)(q^9+1)(q^5+1)} - \frac{18360q^2(\log q)^2}{7\prod_{i=2}^{8}(q^i-1)}$$

and $P_{G,G_0}(2) > 0.999$.

Theorem 6.3.5. *Let $G_0 = \mathrm{E}_8(q)$. Then*

$$P_{G,G_0}(2) \geq 1 - \frac{(46 + \log q)(q-1)}{(q^{30}-1)(q^{12}+1)(q^{10}+1)(q^6+1)} - \frac{21600(\log q)^2}{7(q^8-1)\prod_{i=1}^{7}(q^{2i}-1)}$$

and $P_{G,G_0}(2) > 0.999$.

The probability estimate for $G_0 = \mathrm{F}_4(q)$ from Theorem 6.3.1 is not good enough for $q < 19$. Maximal subgroups of $\mathrm{F}_4(2)$ are given in the Atlas ([39] states that this list is complete). It remains to find better estimates for $\mathrm{F}_4(q)$ when $3 \leq q \leq 17$. Maximal subgroups of $\mathrm{F}_4(q)$, when q is the power of a prime $p \geq 5$ were calculated in [67], and this theorem is given in [92, Theorem 4.4].

Theorem 6.3.6 ([92, Theorem 4.4])**.** *If q is a power of the prime p, $p \geq 5$, then the following are maximal subgroups of $\mathrm{F}_4(q)$.*

1. $[q^{1+14}] : \mathrm{Sp}_6(q).C_{q-1}$
2. $[q^{2+6+12}] : (\mathrm{SL}_2(q) \times \mathrm{SL}_3(q)).C_{q-1}$
3. $[q^{3+2+9+6}] : (\mathrm{SL}_3(q) \times \mathrm{SL}_2(q)).C_{q-1}$
4. $[q^{7+8}] : 2{\cdot}\Omega_7(q).C_{q-1}$
5. $2{\cdot}\Omega_9(q)$
6. $2^{2\cdot}\mathrm{P}\Omega_8^+(q) : S_3$
7. ${}^3\mathrm{D}_4(q) : 3$
8. $(\mathrm{Sp}_6(q) \circ \mathrm{SL}_2(q)).2$
9. $(\mathrm{SL}_3(q) \circ \mathrm{SL}_3(q)).C_{(q-1,3)}.2$
10. $(\mathrm{SU}_3(q) \circ \mathrm{SU}_3(q)).C_{(q+1,3)}.2$

11. $\mathrm{SO}_3(q) \times \mathrm{G}_2(q)$

12. $\mathrm{F}_4(q_0)$*, if* $q = q_0^r$*,* r *prime*

13. $3^3 : \mathrm{SL}_3(q)$*, if* $q = p$

14. $\mathrm{G}_2(q)$*, if* $p = 7$

15. $\mathrm{PGL}_2(q)$*, if* $p \geq 13$ *and* $q \geq 17$

Every other maximal subgroup of $\mathrm{F}_4(q)$ *is the normaliser of a simple subgroup* S *with trivial centraliser, with* S *isomorphic to one of the groups* ${}^3\mathrm{D}_4(2)$*,* $\mathrm{PSL}_3(3)$*,* $\mathrm{PSU}_3(3)$*, or* $\mathrm{PSL}_2(r)$ *for* $r = 7, 8, 9, 13, 17, 25$ *or* 27*.*

It is shown in [67] that there is one conjugacy class of each subgroup 1-14, and from [59] we may deduce that there is one conjugacy class of subgroups of the form $\mathrm{PGL}_2(q)$ for $p \geq 13$, $q \geq 17$. Then we obtain the following estimate for the probability of generating $\mathrm{F}_4(q)$.

Theorem 6.3.7. *Let* $G_0 = \mathrm{F}_4(q)$*, where* q *is the power of a prime* $p \geq 5$*. Then*

$$P_{G_0}(2) \geq 1 - \frac{1}{q^8}$$

and $P_{G_0}(2) > 0.999$*.*

Proof. We use the theorem above and divide our maximal subgroups into two sets, $\mathcal{K}'$ for the set of maximal subgroups M of G_0 which are known and listed up to conjugacy (that is, subgroups 1 – 15 listed above), and $\mathcal{U}'$ for the remaining subgroups which are almost simple (and whose socle is known).

Let $\mathcal{M}'_{\mathcal{K}}$ be a set of conjugacy class representatives for maximal subgroups $M \in \mathcal{K}'$. We use Lemma 3.2.2, and so we bound the following sum

$$\sum_{M \in \mathcal{K}'} \frac{1}{[G_0 : M]^2} = \sum_{M \in \mathcal{M}'_{\mathcal{K}}} \frac{1}{[G_0 : M]}.$$

There are subgroups of the form $\mathrm{F}_4(q_0)$ where $q = q_0^r$ for some prime r. In this case $q_0 \leq q^{\frac{1}{2}}$ and there are at most $\log q$ such subgroups. Then there are at most 14 other conjugacy classes of maximal subgroups in $\mathcal{K}'$, each of index at least q^{15}. Then

$$\sum_{M \in \mathcal{M}'_{\mathcal{K}}} \frac{1}{[G_0 : M]} \leq \frac{15}{q^{15}}.$$

Subgroups $M \in \mathcal{U}'$ are normalisers of simple groups, and the possibilities for simple groups are listed. Note that q is always odd, and so by Table 6.6

$$i(G_0) \leq \frac{5|G_0|}{|\mathrm{SL}_2(q)||\mathrm{Sp}_6(q)|}.$$

Then we use Lemma 3.2.12 with $m = |\mathrm{Aut}({}^3\mathrm{D}_4(2))| = 634\,023\,936$, $s = 6$ to get

$$\begin{aligned}\sum_{M\in\mathcal{U}'} \frac{1}{[G_0:M]^2} &\leq \frac{i(G_0)ms}{|G_0|}\\ &\leq \frac{5ms}{|\mathrm{SL}_2(q)||\mathrm{Sp}_6(q)|}\\ &\leq \frac{5\times 6\times 634023936}{|\mathrm{SL}_2(q)||\mathrm{Sp}_6(q)|}\\ &= \frac{19020718080}{q^{10}(q^2-1)^2(q^4-1)(q^6-1)}\\ &\leq \frac{1}{q^9}.\end{aligned}$$

So

$$P_{G_0}(2) \geq 1 - \Bigg(\sum_{M\in\mathcal{K}'} \frac{1}{[G_0:M]^2} + \sum_{M\in\mathcal{U}'} \frac{1}{[G_0:M]^2}\Bigg) \geq 1 - \frac{1}{q^8}.$$

This is increasing for increasing q, and so for $q \geq 5$, where q is a power of a prime $p \geq 5$, $P_{\mathrm{F}_4(q)}(2) > 0.999$. □

This is sufficient to show $P_{G,G_0}(2) > 0.999$ when $\mathrm{Out}(G_0) = 1$. Note that $\mathrm{Out}(\mathrm{F}_4(q)) = 1$ if and only if q is an odd prime. So when $q = 5, 7, 11, 13, 17$, $P_{G,G_0}(2) > 0.999$. So far we have shown that $P_{G,G_0}(2) > 0.931$ for all exceptional groups G_0 other than $G_0 = \mathrm{F}_4(2)$, $\mathrm{F}_4(3)$, $\mathrm{F}_4(4)$, $\mathrm{F}_4(8)$, $\mathrm{F}_4(9)$, $\mathrm{F}_4(16)$, $\mathrm{E}_6(2)$, ${}^2\mathrm{E}_6(2)$, ${}^2\mathrm{E}_6(3)$, $\mathrm{E}_6(3)$. These groups are considered in the next section.

6.3.1 Probability estimates for $\mathrm{F}_4(2)$, $\mathrm{F}_4(3)$, $\mathrm{F}_4(4)$, $\mathrm{F}_4(8)$, $\mathrm{F}_4(9)$, $\mathrm{F}_4(16)$, $\mathrm{E}_6(2)$, $\mathrm{E}_6(3)$, ${}^2\mathrm{E}_6(2)$ and ${}^2\mathrm{E}_6(3)$

In this section $G_0 \leq G \leq \mathrm{Aut}(G_0)$, where $G_0 = \mathrm{F}_4(q)$, $\mathrm{E}_6(q)$, or ${}^2\mathrm{E}_6(q)$. Again $\mathcal{K}$ and $\mathcal{U}$ are respectively the known and unknown maximal subgroups of G that do not contain G_0. The idea of the proof for the remaining exceptional groups is similar. The same estimates from Lemma 6.2.8 are used for $\sum_{M\in\mathcal{K}} 1/[G:M]^2$ as they are still small. To estimate $\sum_{M\in\mathcal{U}} 1/[G:M]^2$ we use the same ideas as previously, namely bounding $|M|$ for $M \in \mathcal{M}$, and estimating the number of simple subgroups by using the fact they can be generated by an involution and another element. As we are considering particular groups G_0, we may determine all the possibilities for simple subgroups of G_0, and we can find a tighter bound on $|M|$ for $M \in \mathcal{U}$. We denote the set of socles of subgroups in $\mathcal{U}$ by $\mathcal{U}_s$. We may further restrict the possibilities for maximal subgroups of $\mathcal{U}$ in defining characteristic. For these subgroups, if $S = \mathrm{Soc}(M)$, then $\mathrm{rk}(S) \leq \frac{1}{2}\mathrm{rk}(G_0)$.

From [59, Theorem 8] we determine the possibilities for $M \in \mathcal{U}$ in defining characteristic. Note that this includes subgroups from both part (I)(e) and part (VI) of [59, Theorem 8]. We have only included the cases where $G_0 = \mathrm{F}_4(q)$, $\mathrm{E}_6(q)$ or ${}^2\mathrm{E}_6(q)$ as that is all we are considering in this section.

Theorem 6.3.8. *Let $M \in \mathcal{U}$ where $S = \mathrm{Soc}(M)$ is a group of Lie type in defining characteristic. Suppose S is defined over a field of order q_0. Then one of the following holds.*

1. *$q_0 \leq 9$.*
2. *$S = \mathrm{PSL}_3(16)$ or $\mathrm{PSU}_3(16)$.*
3. *$S = \mathrm{PSL}_2(q_0)$, ${}^2\mathrm{B}_2(q_0)$ or ${}^2\mathrm{G}_2(q_0)$ for $q_0 \leq (2, p-1).u(G)$, where $u(G) = 68$ if $G_0 = \mathrm{F}_4(q)$, and $u(G) = 124$ if $G_0 = \mathrm{E}_6(q)$ or ${}^2\mathrm{E}_6(q)$.*
4. *If $G_0 = \mathrm{F}_4(q)$ then $S = \mathrm{PSL}_2(q)$ for $p \geq 13$, or $S = \mathrm{G}_2(q)$ for $p = 7$.*
5. *If $G_0 = \mathrm{E}_6(q)$ then $S = \mathrm{PSL}_3(q)$ for $p \geq 5$, or $S = \mathrm{G}_2(q)$ for $p \neq 7$.*
6. *If $G_0 = {}^2\mathrm{E}_6(q)$ then $S = \mathrm{PSU}_3(q)$ for $p \geq 5$, or $S = \mathrm{G}_2(q)$ for $p \neq 7$.*

Using the ideas of Lemma 3.2.12 we can find a better upper bound on the number of subgroups of G_0 which are isomorphic to a given simple group S. Recall $i(H)$ is the number of involutions of H. Similarly for a prime p, we denote the number of elements of H of order p by $i_p(H)$.

Lemma 6.3.9. *Let S be a simple subgroup of a group H. Suppose S can be generated by an involution t and an element x of order p. Suppose that there are k such pairs $(t, x) \in S \times S$ that generate S. Then the number of subgroups of H isomorphic to S is at most $\frac{i(H)i_p(H)}{k}$.*

Proof. Suppose $(t, x) \in H \times H$ generates a simple group S, where t is an involution and x an element of order p. The number of pairs $(t, x) \in H \times H$ such that $\langle t, x \rangle = S$ is at most $i(H)i_p(H)$. Then we divide by k, as there are k such pairs in $S \times S \subseteq H \times H$ which generate the same subgroup S. □

We already have an estimate for the number of involutions, we now estimate $i_p(H)$.

Lemma 6.3.10. *Let p be a prime such that p divides $|H|$. Let P be a Sylow p-subgroup and let n be the largest divisor of $[H : P]$ such that $n = 1 \mod p$. Then $i_p(H) \leq n(|P| - 1)$.*

Proof. Let x be an element of order p. Then $x \in P$ for some Sylow p-subgroup of H and P contains at most $|P| - 1$ elements of order p. Let n_p be the number of Sylow p-subgroups. Sylow's Theorem tells us that n_p divides $[H : N_H(P)]$ and therefore must divide $[H : P]$. It also gives $n_p = 1 \mod p$. Then $n_p \leq n$ and so $i_p(H) \leq n(|P| - 1)$. □

As described at the start of this section, we wish to bound the number of subgroups of G_0 which are isomorphic to some simple group S. Let S be a simple subgroup of G_0. To use these lemmas we wish to find a prime p such that S is generated by an involution and an element of order p.

If we have a subgroup S of G_0, we choose p to be a prime which divides the order of both S and G_0, but p^2 does not. This is not necessary but this makes it easier to find elements of order p using GAP (we construct a Sylow p-subgroup, and choose any non-identity element). Then we confirm that S is generated by an involution and an element of order p by trial and error. To use Lemma 6.3.9 we determine a lower bound for k computationally using the following method. We choose an element $x \in S$ of order p and determine z, the number of involutions $t \in S$ such that $\langle t, x\rangle = S$. All conjugates $(t^s, x^s) = S$, for $s \in S$, generate S. Then there are $[S : C_S(x)]$ distinct pairs (t^s, x^s) generating S (the number of distinct conjugates of x). Then there are at least $z[S : C_S(x)]$ such pairs in $S \times S$, that is, $k \geq z[S : C_S(x)]$.

The probability of generating an almost simple group with socle $\mathrm{F}_4(3)$

Let G be an almost simple group with socle $G_0 = \mathrm{F}_4(3)$. In this case $\mathrm{Out}(\mathrm{F}_4(3)) = 1$ and so the only possibility for G is $G = \mathrm{F}_4(3)$. We calculate an estimate for $\sum_{M\in\mathcal{U}} 1/[G : M]^2$. First we determine all the possibilities for simple groups in $\mathcal{U}_s$.

Lemma 6.3.11. *Let S be a simple subgroup of $\mathrm{F}_4(3)$, where S is alternating, sporadic, or of Lie type in characteristic other than 3. Then S is isomorphic to one of the following groups:*

$$A_n \text{ for } n \leq 10, \mathrm{J}_2,$$
$$\mathrm{PSL}_2(7), \mathrm{PSL}_2(8), \mathrm{PSL}_2(13), \mathrm{PSL}_2(25),$$
$$\mathrm{PSL}_3(4), \mathrm{PSU}_4(2), \mathrm{PSp}_6(2), {}^3\mathrm{D}_4(2).$$

Then $|\mathrm{Aut}(S)|$ is at most 634 023 936, and $|\mathrm{Aut}(S)||\mathrm{Out}(S)|$ is at most 1 902 071 808.

Proof. The order of $\mathrm{F}_4(3)$ is $2^{15}.3^{24}.5^2.7^2.13^2.41.73$. Possibilities for S come from Theorem 6.2.10, and we eliminate subgroups in characteristic 3 and those whose order does not divide $|\mathrm{F}_4(3)|$. As 11 is not a divisor of $|\mathrm{F}_4(3)|$, S cannot be A_{11}. By looking at the order of the sporadic groups, we see that J_2 is the only one whose order divides $|\mathrm{F}_4(3)|$. Similarly, the groups of Lie type listed are the only ones whose order divides $|\mathrm{F}_4(3)|$. We exclude $\mathrm{P}\Omega_8^+(2)$, as its smallest non-trivial representation in characteristic 3 has degree 28 (from [39]), but $\mathrm{F}_4(3)$ has a representation of degree 25 over $\mathbb{F}_3$ (from [63]), and so $\mathrm{P}\Omega_8^+(2)$ cannot embed in $\mathrm{F}_4(3)$. By looking at the orders of the groups above, we see that both $|\mathrm{Aut}(S)|$ and $|\mathrm{Aut}(S)||\mathrm{Out}(S)|$ are maximal when $S = {}^3\mathrm{D}_4(2)$. □

S	$\lvert S\rvert$	$\lvert\mathrm{Out}(S)\rvert$
$\mathrm{PSL}_2(3^2)$	$2^3.3^2.5$	4
$\mathrm{PSL}_2(3^3)$	$2^2.3^3.7.13$	6
$\mathrm{PSL}_2(3^4)$	$2^4.3^4.5.41$	8
$\mathrm{PSL}_3(3)$	$2^4.3^3.13$	2
$\mathrm{PSL}_3(3^2)$	$2^7.3^6.5.7.13$	4
$\mathrm{PSU}_3(3)$	$2^5.3^3.7$	2
$\mathrm{PSU}_3(3^2)$	$2^5.3^6.5^2.73$	4
$\mathrm{PSp}_4(3)$	$2^6.3^4.5$	4
$\mathrm{PSp}_4(3^2)$	$2^8.3^8.5^2.41$	4
$\mathrm{G}_2(3)$	$2^6.3^6.7$	2

Table 6.7: Possible simple subgroups of Lie type in $\mathrm{F}_4(3)$

Lemma 6.3.12. *Let S be a simple subgroup of $\mathrm{F}_4(3)$, where S is a group of Lie type in characteristic 3 and $\mathrm{rk}(S) \leq 2$. Then S is isomorphic to one of the groups listed in Table 6.7.*

Proof. Groups of Lie type in characteristic 3, whose untwisted rank is at most 2, are of the form $\mathrm{PSL}_2(3^k)$, $\mathrm{PSL}_3(3^k)$, $\mathrm{PSp}_4(3^k)$, $\mathrm{PSU}_3(3^k)$, $\mathrm{G}_2(3^k)$ or ${}^2\mathrm{G}_2(3^k)$. Other groups of Lie type with the correct untwisted rank are either isomorphic to one of the groups listed here or do not occur over fields of characteristic 3. We determine an upper bound on possible values of k using Theorem 6.3.8 and the fact that $|S| \leq 4.3^{20}$ by Theorem 6.2.9. We then consider each possible value of k and see if the order of the subgroup divides $|\mathrm{F}_4(3)|$.

First consider the case where $S = \mathrm{PSL}_2(3^k)$, then we must have $k \leq 4$ by Theorem 6.3.8. When $k = 1$, S is not simple. By Theorem 6.3.8 if $S = \mathrm{PSL}_3(3^k)$, $\mathrm{PSU}_3(3^k)$ or $\mathrm{PSp}_4(3^k)$ then $k \leq 2$.

If $S = \mathrm{G}_2(3^k)$ then $k = 1$ otherwise the group is too large by Theorem 6.2.9. Finally we consider the case where $S = {}^2\mathrm{G}_2(3^k)$. Then $k = 2m+1$ and we must have $m = 1$ otherwise S is too large. But the order of ${}^2\mathrm{G}_2(3^3)$ does not divide $|\mathrm{F}_4(3)|$ and so we do not have any subgroups S of this form. □

Lemma 6.3.13. *Let $\mathcal{S}'$ be the set of the simple groups in $\mathcal{U}_s$ excluding $\mathrm{PSp}_4(9)$. Then*

$$\sum_{\substack{M\in\mathcal{U}\\ \mathrm{Soc}(M)\in\mathcal{S}'}} \frac{1}{[\mathrm{F}_4(3) : M]^2} \leq \frac{7}{162}.$$

Proof. By Lemmas 6.3.11 and 6.3.12 we know what the possibilities for $S \in \mathcal{S}'$ are. Then an upper bound for $|\mathrm{Aut}(S)||\mathrm{Out}(S)|$ for $S \in \mathcal{S}'$ is $c = 1\,902\,071\,808$ (corresponding to $S = {}^3\mathrm{D}_4(2)$). Using Table 6.6 the number

of involutions is bounded above by

$$i(\mathrm{F}_4(3)) \leq 5[\mathrm{F}_4(3) : C_{\mathrm{F}_4(3)}(t)] \leq \frac{5|\mathrm{F}_4(3)|}{|\mathrm{SL}_2(3)||\mathrm{Sp}_6(3)|},$$

where t is an involution in a conjugacy class of maximal size. Then by Lemma 3.2.12,

$$\begin{aligned}\sum_{\substack{M\in\mathcal{U}\\ \mathrm{Soc}(M)\in\mathcal{S}'}} \frac{1}{[\mathrm{F}_4(3) : M]^2} &\leq \frac{i(\mathrm{F}_4(3))c}{|\mathrm{F}_4(3)|}\\ &\leq \frac{5c}{|\mathrm{SL}_2(3)||\mathrm{Sp}_6(3)|}\\ &= \frac{7}{162}.\end{aligned}$$

□

Lemma 6.3.14. *Let $\mathcal{S}'$ be the set of simple subgroups in $\mathcal{U}_s$ which are isomorphic to* $\mathrm{PSp}_4(9)$*. Then*

$$\sum_{\substack{M\in\mathcal{U}\\ \mathrm{Soc}(M)\in\mathcal{S}'}} \frac{1}{[\mathrm{F}_4(3) : M]^2} \leq \frac{125}{23823072}.$$

Proof. The order of $\mathrm{PSp}_4(9)$ is $1\,721\,606\,400$ and $|\mathrm{Out}(\mathrm{PSp}_4(9))| = 4$. We use Lemma 6.3.9 to bound the number of such subgroups in $\mathrm{F}_4(3)$. Using Magma [8], we choose an element $x \in \mathrm{PSp}_4(9)$ of order 41, and determine the number of involutions t such that $\langle t, x\rangle$ generates $\mathrm{PSp}_4(9)$. There are 298152 such involutions for our choice of x. The centraliser of x in $\mathrm{PSp}_4(9)$ has order 41. Then there are at least

$$298152[\mathrm{PSp}_4(9) : C_{\mathrm{PSp}_4(9)}(x)] = 298152|\mathrm{PSp}_4(9)|/41 = 7272|\mathrm{PSp}_4(9)|$$

pairs of right form, that is, $k \geq 7272|\mathrm{PSp}_4(9)|$.

The number of involutions is bounded by

$$i(\mathrm{F}_4(3)) \leq 5[\mathrm{F}_4(3) : C_{\mathrm{F}_4(3)}(t)]$$

where $|C_{\mathrm{F}_4(3)}(t)|$ is as in Table 6.6. Next we estimate $i_{41}(\mathrm{F}_4(3))$. Let P be a Sylow 41-subgroup. The largest divisor of $[\mathrm{F}_4(3) : P]$ congruent to 1 mod 41 is $\frac{|\mathrm{F}_4(3)|}{2^4.41}$. Then

$$i_{41}(\mathrm{F}_4(3)) \leq \frac{40|\mathrm{F}_4(3)|}{2^4.41}$$

by Lemma 6.3.10. The bound on the number of subgroups in $\mathcal{S}'$ from Lemma 6.3.9 becomes

$$\frac{i(\mathrm{F}_4(3))i_{41}(\mathrm{F}_4(3))}{k} \leq \frac{200|\mathrm{F}_4(3)|^2}{4770432|\mathrm{SL}_2(3)||\mathrm{Sp}_6(3)|}.$$

We use this to estimate the sum for maximal subgroups M with socle $\mathrm{PSp}_4(9)$,

$$\begin{aligned}\sum_{\substack{M\in\mathcal{U}\\ \mathrm{Soc}(M)\in\mathcal{S}'}} \frac{1}{[\mathrm{F}_4(3):M]^2} &\leq \frac{|\mathrm{Aut}(\mathrm{PSp}_4(9))|^2}{|\mathrm{F}_4(3)|^2}\times\frac{200|\mathrm{F}_4(3)|^2}{4770432|\mathrm{SL}_2(3)||\mathrm{Sp}_6(3)|}\\ &\leq \frac{200|\mathrm{PSp}_4(9)||\mathrm{Out}(\mathrm{PSp}_4(9))|^2}{4770432|\mathrm{SL}_2(3)||\mathrm{Sp}_6(3)|}\\ &= \frac{125}{23823072}\end{aligned}$$

□

Lemma 6.3.15. *Let $G_0 = \mathrm{F}_4(3)$. Then $P_{G,G_0}(2) > 0.956$.*

Proof. The only almost simple group G with socle G_0 is $\mathrm{F}_4(3)$ itself. Lemma 6.2.8 bounds $\sum_{M\in\mathcal{K}} 1/[G:M]$. By Lemmas 6.3.13 and 6.3.14 above,

$$\sum_{M\in\mathcal{U}}\frac{1}{[G:M]^2}\leq\frac{7}{162}+\frac{125}{23823072}.$$

Then by Lemma 3.2.2,

$$P_{G,G_0}(2)\geq 1-\left(\sum_{M\in\mathcal{K}}\frac{1}{[G:M]^2}+\sum_{M\in\mathcal{U}}\frac{1}{[G:M]^2}\right)>0.956.$$

□

The probability of generating an almost simple group with socle $\mathrm{F}_4(4)$

Now let G be an almost simple group with socle $G_0 = \mathrm{F}_4(4)$. First we determine the possibilities for $S\in\mathcal{U}_s$.

Lemma 6.3.16. *Let S be a simple subgroup of $\mathrm{F}_4(4)$, where S is alternating, sporadic, or of Lie type in odd characteristic. Then S is isomorphic to one of the following groups:*

$$\begin{array}{l}A_n \text{ for } n\leq 10, \mathrm{J}_2,\\ \mathrm{PSL}_2(13), \mathrm{PSL}_2(17), \mathrm{PSL}_2(25), \mathrm{PSL}_2(27),\\ \mathrm{PSL}_3(3), \mathrm{PSL}_4(3), \mathrm{PSU}_3(3), \mathrm{PSp}_4(3).\end{array}$$

Then $|\mathrm{Aut}(S)|$ is at most $24\,261\,120$ and $|\mathrm{Aut}(S)||\mathrm{Out}(S)|$ is at most $97\,044\,480$.

Proof. A simple subgroup S of $\mathrm{F}_4(4)$ must be one of the groups listed in Theorem 6.2.10. We consider all possible groups S from these lemmas and we eliminate any subgroups in characteristic 2. The order of $\mathrm{F}_4(4)$ is $2^{48}.3^6.5^4.7^2.13^2.17^2.241.257$. Then, out of all remaining possibilities for S, we only include those whose order divides $|F_4(4)|$. We are left with the possibilities for S listed above. We see that both $|\mathrm{Aut}(S)|$ and $|\mathrm{Aut}(S)||\mathrm{Out}(S)|$ are largest when $S = \mathrm{PSL}_4(3)$. □

Lemma 6.3.17. *Let S be a simple subgroup of $\mathrm{F}_4(4)$ where S is a subgroup of Lie type in characteristic 2 and $\mathrm{rk}(S) \leq 2$. Then S is isomorphic to one of the following:*

$$\mathrm{PSL}_2(2^2), \mathrm{PSL}_2(2^3), \mathrm{PSL}_2(2^4), \mathrm{PSL}_2(2^6),$$
$$\mathrm{PSL}_3(2), \mathrm{PSL}_3(2^2), \mathrm{PSL}_3(2^4), \mathrm{PSU}_3(2^2),$$
$$\mathrm{PSU}_3(2^4), \mathrm{PSp}_4(2^2), \mathrm{PSp}_4(2^3), {}^2\mathrm{B}_2(2^3), \mathrm{G}_2(2^2).$$

and $|\mathrm{Aut}(S)||\mathrm{Out}(S)| \leq 821\,211\,955\,200$.

Proof. Groups of Lie type in characteristic 2, whose untwisted rank is at most 2, are of the form $\mathrm{PSL}_2(2^k)$, $\mathrm{PSL}_3(2^k)$, $\mathrm{PSp}_4(2^k)$, $\mathrm{PSU}_3(2^k)$, ${}^2\mathrm{B}_2(2^k)$ or $\mathrm{G}_2(2^k)$. Other groups of Lie type with the correct untwisted rank, are either isomorphic to one of the groups listed here, or do not occur over fields of characteristic 2. Theorem 6.3.8 determines the values for k in each case. We also require that the order of S divides $|\mathrm{F}_4(4)|$. The order of $\mathrm{F}_4(4)$ is $2^{24}.3^6.5^4.7^2.13^2.17^2.241.257$.

First consider $S = \mathrm{PSL}_2(2^k)$. Then $k \leq 6$ by Theorem 6.3.8. When $k = 5$, the order of S does not divide $|\mathrm{F}_4(4)|$ and when $k = 1$, S is not simple. So we are left with the possibilities above.

Next consider $S = \mathrm{PSL}_3(2^k)$. Then $k \leq 4$ by Theorem 6.3.8. We rule out $k = 3$ as in this case $|S|$ does not divide $|\mathrm{F}_4(4)|$. When $S = \mathrm{PSU}_3(2^k)$ then by Theorem 6.3.8, $k \leq 4$. We rule out the possibility $k = 3$ as in this cases $|S|$ does not divide $|\mathrm{F}_4(4)|$. If $k = 1$ then S is not simple, and so we are left with the possibilities listed above.

Next consider $S = \mathrm{PSp}_4(2^k)$. Then we require $k \leq 3$ by Theorem 6.3.8, and we must have $k > 1$ for S to be simple. Now let $S = {}^2\mathrm{B}_2(2^k)$. Then k must be odd and greater than 3. By Theorem 6.3.8 we must have $k \leq 5$. The only time $|S|$ divides $|\mathrm{F}_4(4)|$ is when $k = 3$.

Finally consider $S = \mathrm{G}_2(2^k)$. Then $k \neq 1$ as $\mathrm{G}_2(2)$ is not simple. We require $k \leq 3$ by Theorem 6.3.8. When $k = 3$, $|S|$ does not divide $|\mathrm{F}_4(4)|$. Then the only possibility is $S = \mathrm{G}_2(2^2)$.

From the possibilities for S listed above, $|\mathrm{Aut}(S)||\mathrm{Out}(S)|$ is maximal when $S = \mathrm{PSL}_3(2^4)$. □

Lemma 6.3.18. *Let G be an almost simple group with socle $\mathrm{F}_4(4)$. Then*

$$\sum_{M \in \mathcal{U}} \frac{1}{[G : M]^2} \leq \frac{69615}{4194304}.$$

Proof. The possibilities for $S \in \mathcal{U}_s$ come from Lemmas 6.3.16 and 6.3.17. For $S \in \mathcal{U}_s$, we bound $|\mathrm{Aut}(S)||\mathrm{Out}(S)|$ by $c = |\mathrm{Aut}(\mathrm{PSL}_3(2^4))||\mathrm{Out}(\mathrm{PSL}_3(2^4)|$. We estimate the number of involutions by $i(\mathrm{F}_4(4)) \leq 5[\mathrm{F}_4(4) : C_{\mathrm{F}_4(4)}(t)]$ where $|C_{\mathrm{F}_4(4)}(t)| = 4^{18}|\mathrm{SL}_2(4)|^2$ from Table 6.6. Then by Lemma 3.2.12,

$$\begin{aligned}\sum_{M\in\mathcal{U}} \frac{1}{[G:M]^2} &\leq \frac{i(\mathrm{F}_4(4))c}{|\mathrm{F}_4(4)|} \\ &\leq \frac{5c}{4^{18}\times 60^2} \\ &\leq \frac{69615}{4194304}.\end{aligned}$$

□

Lemma 6.3.19. *Let G be an almost simple group with socle $\mathrm{F}_4(4)$. Then $P_{G,\mathrm{F}_4(4)}(2) > 0.983$.*

Proof. Lemma 6.2.8 bounds $\sum_{M\in\mathcal{K}} 1/[G:M]^2$. By Lemma 6.3.18,

$$\sum_{M\in\mathcal{U}} \frac{1}{[G:M]^2} \leq \frac{69615}{4194304}.$$

Then by Lemma 3.2.6,

$$P_{G,G_0}(2) \geq 1 - \left(\sum_{M\in\mathcal{K}} \frac{1}{[G:M]^2} + \sum_{M\in\mathcal{U}} \frac{1}{[G:M]^2} \right) > 0.983.$$

□

The probability of generating an almost simple group with socle $\mathrm{F}_4(8)$

Let G be an almost simple group with socle $G_0 = \mathrm{F}_4(8)$. First we bound $\sum_{M\in\mathcal{U}} 1/[G:M]^2$, and so we begin by determining the possibilities for $S \in \mathcal{U}_s$.

Lemma 6.3.20. *Let S be a simple subgroup of $\mathrm{F}_4(8)$, where S is alternating, sporadic, or of Lie type in odd characteristic. Then S is isomorphic to one of the following groups:*

$$\begin{array}{l} A_n \text{ for } n \leq 10, \mathrm{J}_2, \\ \mathrm{PSL}_2(13), \mathrm{PSL}_2(17), \mathrm{PSL}_2(25), \mathrm{PSL}_2(27), \\ \mathrm{PSL}_3(3), \mathrm{PSL}_4(3), \mathrm{PSU}_3(3). \end{array}$$

Then $|\mathrm{Aut}(S)|$ is at most 24 261 120 and $|\mathrm{Aut}(S)||\mathrm{Out}(S)|$ is at most 97 044 480.

Proof. The order of $\mathrm{F}_4(8)$ is $2^{72}.3^{10}.5^2.7^4.13^2.17.19^2.37.73^2.109.241$. Possiblities for $S < \mathrm{F}_4(8)$ where S is alternating, sporadic, or of Lie type in cross characteristic, come from Theorem 6.2.10. We exclude subgroups S whose order does not divide $|\mathrm{F}_4(8)|$ and those in characteristic 2, leaving us with the list above. Then $|\mathrm{Aut}(S)|$ and $|\mathrm{Aut}(S)||\mathrm{Out}(S)|$ take their largest values when $S = \mathrm{PSL}_4(3)$. □

Lemma 6.3.21. *Let S be a simple subgroup of $\mathrm{F}_4(8)$, where S is of Lie type in characteristic 2 such that $\mathrm{rk}(S) \leq 2$. Then S is isomorphic to one of the following:*

$$\begin{array}{l}\mathrm{PSL}_2(2^3), \mathrm{PSL}_2(2^3), \mathrm{PSL}_2(2^4), \mathrm{PSL}_2(2^6),\\ \mathrm{PSL}_3(2), \mathrm{PSL}_3(2^2), \mathrm{PSL}_3(2^3), \mathrm{PSL}_3(2^4),\\ \mathrm{PSU}_3(2^2), \mathrm{PSU}_3(2^3), \mathrm{PSp}_4(2^2), \mathrm{PSp}_4(2^3),\\ {}^2\mathrm{B}_2(2^3), \mathrm{G}_2(2^2), \mathrm{G}_2(2^3),\end{array}$$

and $|\mathrm{Aut}(S)||\mathrm{Out}(S)| \leq 38\,963\,794\,673\,664$.

Proof. Theorem 6.3.8 gives the possible simple subgroups S of $\mathrm{F}_4(8)$. These subgroups S are isomorphic to one of the following: $\mathrm{PSL}_2(2^k)$ for $k \leq 6$; $\mathrm{PSL}_3(2^k)$ for $k \leq 4$; $\mathrm{PSp}_4(2^k)$ for $k \leq 3$; $\mathrm{PSU}_3(2^k)$ for $k \leq 4$; ${}^2\mathrm{B}_2(2^k)$ for $k \leq 5$; $\mathrm{G}_2(2^k)$ for $k \leq 3$. As $|S|$ must divide $|\mathrm{F}_4(8)|$ the remaining possibilities for S are those listed above. We see that in all cases $|\mathrm{Aut}(S)||\mathrm{Out}(S)|$ is largest when $S = \mathrm{G}_2(8)$. □

Lemma 6.3.22. *Let G be an almost simple group with socle $\mathrm{F}_4(8)$. Then*

$$\sum_{M \in \mathcal{U}} \frac{1}{[G : M]^2} \leq 0.0001$$

Proof. From Lemmas 6.3.20 and 6.3.21, for $S \in \mathcal{U}_s$, $|\mathrm{Aut}(S)||\mathrm{Out}(S)|$ takes its largest value when $S = \mathrm{G}_2(8)$. So take $c = 3^2|\mathrm{G}_2(8)|$. If t is an involution in a conjugacy class of maximal size, using Table 6.6 we estimate the number of involutions by

$$i(\mathrm{F}_4(8)) \leq 5[\mathrm{F}_4(8) : C_{\mathrm{F}_4(8)}(t)] \leq \frac{5|\mathrm{F}_4(8)|}{8^{18}|\mathrm{SL}_2(8)|^2}.$$

Then, by Lemma 3.2.12,

$$\begin{aligned}\sum_{\substack{M \in \mathcal{U}\\ \mathrm{Soc}(M) \in \mathcal{S}'}} \frac{1}{[G : M]^2} &\leq \frac{i(\mathrm{F}_4(8))c}{|\mathrm{F}_4(8)|}\\ &\leq \frac{5c}{|C_{\mathrm{F}_4(8)}(t)|}\\ &\leq \frac{5.3^2|\mathrm{G}_2(8)|}{8^{18}|\mathrm{SL}_2(8)|^2}\\ &\leq 0.0001.\end{aligned}$$

□

We may now estimate the probability $P_{G,G_0}(2)$.

Lemma 6.3.23. *Let G be an almost simple group with socle $\mathrm{F}_4(8)$. Then $P_{G,\mathrm{F}_4(8)}(2) > 0.999$.*

Proof. Using the estimates from Lemmas 6.2.8 and 6.3.22,

$$\sum_{\substack{M<_{\max}G \\ G_0 \not\leq M}} \frac{1}{[G:M]^2} \leq 0.0001.$$

Then by Lemma 3.2.6 $P_{G,\mathrm{F}_4(8)}(2) > 0.999$. □

The probability of generating an almost simple group with socle $\mathrm{F}_4(9)$

Let G be an almost simple group with socle $G_0 = \mathrm{F}_4(9)$. First we determine possibilities for $S \in \mathcal{U}_s$.

Lemma 6.3.24. *Let S be a simple subgroup of $\mathrm{F}_4(9)$, where S is alternating, sporadic, or of Lie type in characteristic other than 3. Then S is isomorphic to one of the following groups:*

$$\begin{array}{l} A_n \text{ for } n \leq 10, \mathrm{J}_2, \\ \mathrm{PSL}_2(7), \mathrm{PSL}_2(8), \mathrm{PSL}_2(13), \mathrm{PSL}_2(17), \\ \mathrm{PSL}_2(25), \mathrm{PSL}_3(4), \mathrm{PSL}_4(2), \mathrm{PSp}_6(2), \\ \mathrm{P\Omega}_8^+(2), {}^3\mathrm{D}_4(2). \end{array}$$

Then $|\mathrm{Aut}(S)|$ is at most $1\,045\,094\,400$, and $|\mathrm{Aut}(S)||\mathrm{Out}(S)|$ is at most $6\,270\,566\,400$.

Proof. Possibilities for S come from Theorem 6.2.10. The order of $\mathrm{F}_4(9)$ is $2^{19}.3^{48}.5^4.7^2.13^2.17.41^2.73^2.193.6481$. We eliminate any subgroups S whose order does not divide $\mathrm{F}_4(9)$, and also those in characteristic 3. From the remaining possibilities for S listed above, we see that both $|\mathrm{Aut}(S)|$ and $|\mathrm{Aut}(S)||\mathrm{Out}(S)|$ take their maximum value when $S = \mathrm{P\Omega}_8^+(2)$. □

Lemma 6.3.25. *Let S be a simple subgroup of $\mathrm{F}_4(9)$, where S is of Lie type in characteristic 2 such that $\mathrm{rk}(S) \leq 2$. Then S is isomorphic to one of the following:*

$$\begin{array}{l} \mathrm{PSL}_2(3^k) \text{ for } k \leq 4, \\ \mathrm{PSL}_3(3^k) \text{ for } k \leq 2, \\ \mathrm{PSU}_3(3^k) \text{ for } k \leq 2, \\ \mathrm{PSp}_4(3^k) \text{ for } k \leq 2, \\ \mathrm{G}_2(3^k) \text{ for } k \leq 2, \end{array}$$

and $|\mathrm{Aut}(S)||\mathrm{Out}(S)| \leq 90\,377\,281\,612\,800$.

Proof. Theorem 6.3.8 gives possibilities for S. Then S is isomorphic to one of the following: $\mathrm{PSL}_2(3^k)$ for $k \leq 4$; $\mathrm{PSL}_3(3^k)$ for $k \leq 2$; $\mathrm{PSU}_3(3^k)$ for $k \leq 2$; $\mathrm{PSp}_4(3^k)$ for $k \leq 2$; $\mathrm{G}_2(3^k)$ for $k \leq 2$; ${}^2\mathrm{G}_2(3^3)$. The order of $\mathrm{F}_4(9)$ is $2^{19}.3^{48}.5^4.7^2.13^2.17.41^2.73^2.193.6481$. As $|S|$ must divide $|\mathrm{F}_4(9)|$ we rule out the possibility ${}^2\mathrm{G}_2(3^3)$. Then $|\mathrm{Aut}(S)||\mathrm{Out}(S)| \leq |\mathrm{Aut}(\mathrm{G}_2(9))||\mathrm{Out}(\mathrm{G}_2(9))|$. □

Lemma 6.3.26. *Let G be an almost simple group with socle $\mathrm{F}_4(9)$. Then*

$$\sum_{M \in \mathcal{U}} \frac{1}{[G:M]^2} \leq \frac{1}{172160640}.$$

Proof. Possibilities for $S \in \mathcal{S}$ come from Theorem 6.2.10 and Lemma 6.3.25. We use Lemma 3.2.12 with $c = |\mathrm{Aut}(\mathrm{G}_2(9))||\mathrm{Out}(\mathrm{G}_2(9))|$. For an involution t in a conjugacy class of maximal size we use $|C_{\mathrm{F}_4(9)}(t)| = |\mathrm{SL}_2(9)||\mathrm{Sp}_6(9)|$ from Table 6.6 and we estimate $i(\mathrm{F}_4(9)) \leq 5[G : C_{\mathrm{F}_4(9)}(t)]$. Then, by Lemma 3.2.12,

$$\begin{aligned}
\sum_{M \in \mathcal{U}} \frac{1}{[G:M]^2} &\leq \frac{i(\mathrm{F}_4(9))c}{|\mathrm{F}_4(9)|} \\
&\leq \frac{5c}{|C_{\mathrm{F}_4(9)}(t)|} \\
&\leq \frac{5c}{|\mathrm{SL}_2(9)||\mathrm{Sp}_6(9)|} \\
&\leq \frac{1}{172160640}.
\end{aligned}$$

□

Then, we may bound the probability.

Lemma 6.3.27. *Let G be an almost simple group with socle $\mathrm{F}_4(9)$. Then $P_{G,\mathrm{F}_4(9)}(2) > 0.999$.*

Proof. Lemma 6.2.8 bounds $\sum_{M \in \mathcal{K}} 1/[G:M]^2$, and Lemma 6.3.26 bounds $\sum_{M \in \mathcal{U}} 1/[G:M]^2$. By Lemma 3.2.6,

$$P_{G,\mathrm{F}_4(9)}(2) \geq 1 - \left(\sum_{M \in \mathcal{K}} \frac{1}{[G:M]^2} + \sum_{M \in \mathcal{U}} \frac{1}{[G:M]^2} \right) > 0.999.$$

□

The probability of generating an almost simple group with socle $\mathrm{F}_4(16)$

Let G be an almost simple group with socle $G_0 = \mathrm{F}_4(16)$. We wish to estimate $\sum_{M \in \mathcal{U}} 1/[G:M]^2$ and so we determine possibilities for $S \in \mathcal{U}_s$.

Lemma 6.3.28. *Let S be a simple subgroup of $\mathrm{F}_4(16)$, where S is alternating, sporadic, or of Lie type in characteristic other than 2. Then S is isomorphic to one of the following groups:*

$$A_n \text{ for } n \leq 10, \mathrm{J}_2,$$
$$\mathrm{PSL}_2(13), \mathrm{PSL}_2(17), \mathrm{PSL}_2(25), \mathrm{PSL}_2(27),$$
$$\mathrm{PSL}_3(3), \mathrm{PSL}_4(3), \mathrm{PSU}_3(3).$$

Then $|\mathrm{Aut}(S)|$ is at most $24\,261\,120$ and $|\mathrm{Aut}(S)||\mathrm{Out}(S)|$ is at most $97\,044\,480$.

Proof. Possibilities for S come from Theorem 6.2.10. The order of $\mathrm{F}_4(16)$ is $2^{96}.3^6.5^4.7^2.13^2.17^4.97.241^2.257^2.673.65537$. Then we eliminate all those possibilities for S whose order does not divide $|\mathrm{F}_4(16)|$. We also remove all subgroups of characteristic 2, and then we are left with the possibilities for S given above. By calculating the orders of each possible S, together with the order of $\mathrm{Out}(S)$, we see that both $|\mathrm{Aut}(S)|$ and $|\mathrm{Aut}(S)||\mathrm{Out}(S)|$ are largest when $S = \mathrm{PSL}_4(3)$. □

Lemma 6.3.29. *Let S be a simple subgroup of $\mathrm{F}_4(16)$, where S is of Lie type in characteristic 2 such that $\mathrm{rk}(S) \leq 2$. Then S is isomorphic to one of the following:*

$$\mathrm{PSL}_2(2^k) \text{ for } k \leq 6,$$
$$\mathrm{PSL}_3(2^k) \text{ for } k \leq 4,$$
$$\mathrm{PSU}_3(2^k) \text{ for } k \leq 4,$$
$$\mathrm{PSp}_4(2^k) \text{ for } k \leq 3,$$
$$\mathrm{G}_2(2^k) \text{ for } k \leq 3,$$
$${}^2\mathrm{B}_2(2^3),$$

and $|\mathrm{Aut}(S)||\mathrm{Out}(S)| \leq 38\,963\,794\,673\,664$.

Proof. Possibilities for subgroups S come from Theorem 6.3.8. The order of $\mathrm{F}_4(16)$ is $2^{96}.3^6.5^4.7^2.13^2.17^4.97.241^2.257^2.673.65537$. As $|S|$ must divide $|\mathrm{F}_4(16)|$ we rule out the possibility $S = {}^2\mathrm{B}_2(2^5)$. The bound from Theorem 6.2.9 means we rule out $S = \mathrm{G}_2(2^4)$. Then we are left with the possibilities for S listed above. Then $|\mathrm{Aut}(S)||\mathrm{Out}(S)|$ is maximal when $S = \mathrm{G}_2(8)$. □

Lemma 6.3.30. *Let G be an almost simple group with socle $\mathrm{F}_4(16)$. Then*

$$\sum_{M \in \mathcal{U}} \frac{1}{[G : M]^2} < 0.0001.$$

Proof. Possibilities for $S \in \mathcal{S}$ come from Lemmas 6.3.28 and 6.3.29. We use Lemma 3.2.12 with $c = |\mathrm{Aut}(\mathrm{G}_2(8))||\mathrm{Out}(\mathrm{G}_2(8))|$. For an involution t in

a conjugacy class of maximal size we use $|C_{\mathrm{F}_4(9)}(t)| = 16^{18}|\mathrm{SL}_2(16)|^2$ from Table 6.6 and we estimate $i(\mathrm{F}_4(16)) \leq 5[G : C_{\mathrm{F}_4(16)}(t)]$. Then,

$$\begin{aligned}\sum_{M\in\mathcal{U}} \frac{1}{[G:M]^2} &\leq \frac{i(\mathrm{F}_4(16))c}{|\mathrm{F}_4(16)|}\\ &\leq \frac{5c}{16^{18}|\mathrm{SL}_2(16)|^2}\\ &< 0.0001.\end{aligned}$$

□

Then we may bound the probability.

Lemma 6.3.31. *Let G be an almost simple group with socle $\mathrm{F}_4(16)$. Then $P_{G,\mathrm{F}_4(16)}(2) > 0.999$.*

Proof. Lemma 6.2.8 bounds $\sum_{M\in\mathcal{K}} 1/[G:M]^2$, and Lemma 6.3.30 bounds $\sum_{M\in\mathcal{U}} 1/[G:M]^2$. Then by Lemma 3.2.6,

$$P_{G,\mathrm{F}_4(16)}(2) \geq 1 - \left(\sum_{M\in\mathcal{K}} \frac{1}{[G:M]^2} + \sum_{M\in\mathcal{U}} \frac{1}{[G:M]^2}\right) > 0.999.$$

□

The probability of generating an almost simple group with socle $\mathrm{E}_6(3)$

Let G be an almost simple group with socle $G_0 = \mathrm{E}_6(3)$. We wish to estimate $\sum_{M\in\mathcal{U}} 1/[G:M]^2$ and so we determine possibilities for $S \in \mathcal{U}_s$.

Lemma 6.3.32. *Let S be a simple subgroup of $\mathrm{E}_6(3)$, where S is alternating, sporadic, or of Lie type in characteristic other than 3. Then S is isomorphic to one of the following groups:*

$$\begin{array}{l} A_n \text{ for } n \leq 12, \mathrm{M}_{11}, \mathrm{M}_{12}, \mathrm{J}_2,\\ \mathrm{PSL}_2(7), \mathrm{PSL}_2(8), \mathrm{PSL}_2(11), \mathrm{PSL}_2(13),\\ \mathrm{PSL}_2(25), \mathrm{PSL}_3(4), \mathrm{PSp}_6(2), \mathrm{P\Omega}_8^+(2),\\ {}^3\mathrm{D}_4(2), {}^2\mathrm{F}_4(2)'.\end{array}$$

Then $|\mathrm{Aut}(S)|$ is at most 1 045 094 400 and $|\mathrm{Aut}(S)||\mathrm{Out}(S)|$ is at most 6 270 566 400.

Proof. Possibilities for S come from Theorem 6.2.10. The order of $\mathrm{E}_6(3)$ is $2^{17}.3^{36}.5^2.7^2.11^2.13^3.41.73.757$. We rule out subgroups S whose order does not divide $|\mathrm{E}_6(3)|$, and also those subgroups which are of characteristic 3. Then the remaining possibilities for S are those listed above, and the largest value of both $|\mathrm{Aut}(S)|$ and $|\mathrm{Aut}(S)||\mathrm{Out}(S)|$ corresponds to $S = \mathrm{P\Omega}_8^+(2)$. □

Lemma 6.3.33. *Let S be a simple subgroup of $\mathrm{E}_6(3)$, where S is of Lie type in characteristic 2 such that $\mathrm{rk}(S) \leq 3$. Then S is isomorphic to one of the following:*

$$\mathrm{PSL}_2(3^k) \text{ for } k \leq 5,$$
$$\mathrm{PSL}_3(3^k) \text{ for } k \leq 2,$$
$$\mathrm{PSL}_4(3^k) \text{ for } k \leq 2,$$
$$\mathrm{PSU}_3(3^k) \text{ for } k \leq 2,$$
$$\mathrm{PSp}_4(3^k) \text{ for } k \leq 2,$$
$$\mathrm{G}_2(3^k) \text{ for } k \leq 2,$$
$$\mathrm{PSU}_4(3), \mathrm{PSp}_6(3), \Omega_7(3), \mathrm{P}\Omega_8^-(3),$$

and $|\mathrm{Aut}(S)||\mathrm{Out}(S)| \leq 12\,994\,519\,832\,985\,600$.

Proof. Theorem 6.3.8 gives possibilities for S. Theorem 6.2.9 allows us to rule out more possibilities as we require $|S| \leq 4.3^{28}$. The order of $\mathrm{E}_6(3)$ is $2^{17}.3^{36}.5^2.7^2.11^2.13^2.13^3.41.73.757$ and we rule out subgroups whose order does not divide $|\mathrm{E}_6(3)|$. Then we are left with the possibilities above. In all cases $|\mathrm{Aut}(S)||\mathrm{Out}(S)|$ is maximal when $S = \mathrm{PSL}_4(9)$. □

Lemma 6.3.34. *Let G be an almost simple group with socle $\mathrm{E}_6(3)$. Then*

$$\sum_{M \in \mathcal{U}} \frac{1}{[G:M]^2} \leq \frac{8200}{127413}.$$

Proof. Possibilities for $S \in \mathcal{S}$ come from Lemma 6.3.32 and Lemma 6.3.33. We use Lemma 3.2.12 with $c = |\mathrm{Aut}(\mathrm{PSL}_4(9))||\mathrm{Out}(\mathrm{PSL}_4(9))|$. For an involution t in a conjugacy class of maximal size $|C_{\mathrm{E}_6(3)}(t)| = |\mathrm{SL}_2(3)||\mathrm{SL}_6(3)|$ by Table 6.6 and we estimate $i(\mathrm{E}_6(3)) \leq 5[G : C_{\mathrm{E}_6(3)}(t)]$. Then,

$$\begin{aligned}\sum_{M \in \mathcal{U}} \frac{1}{[G:M]^2} &\leq \frac{i(\mathrm{E}_6(3))c}{|\mathrm{E}_6(3)|} \\ &\leq \frac{5c}{|\mathrm{SL}_2(3)||\mathrm{SL}_6(3)|} \\ &= \frac{8200}{127413}.\end{aligned}$$

□

Then, we may bound the probability.

Lemma 6.3.35. *Let G be an almost simple group with socle $\mathrm{E}_6(3)$. Then $P_{G,\mathrm{E}_6(3)}(2) > 0.935$.*

Proof. Lemma 6.2.8 bounds $\sum_{M \in \mathcal{K}} 1/[G:M]^2$, and Lemma 6.3.34 bounds $\sum_{M \in \mathcal{U}} 1/[G:M]^2$. Then by Lemma 3.2.6,

$$P_{G,\mathrm{E}_6(3)}(2) \geq 1 - \left(\sum_{M \in \mathcal{K}} \frac{1}{[G:M]^2} + \sum_{M \in \mathcal{U}} \frac{1}{[G:M]^2} \right) > 0.935.$$

□

The probability of generating an almost simple group with socle ${}^2\mathrm{E}_6(3)$

Let G be an almost simple group with socle $G_0 = {}^2\mathrm{E}_6(3)$. We wish to estimate $\sum_{M\in\mathcal{U}} 1/[G:M]^2$ and so we determine possibilities for $S \in \mathcal{U}_s$.

Lemma 6.3.36. *Let S be a simple subgroup of ${}^2\mathrm{E}_6(3)$, where S is alternating, sporadic, or of Lie type in characteristic other than 3. Then S is isomorphic to one of the following groups:*

$$\begin{array}{l} A_n \text{ for } n \leq 10, \mathrm{J}_2, \\ \mathrm{PSL}_2(7), \mathrm{PSL}_2(8), \mathrm{PSL}_2(13), \mathrm{PSL}_2(19), \\ \mathrm{PSL}_2(25), \mathrm{PSL}_3(4), \mathrm{PSU}_3(4), \mathrm{PSp}_6(2), \\ \mathrm{P}\Omega_8^+(2), {}^3\mathrm{D}_4(2), {}^2\mathrm{F}_4(2)'. \end{array}$$

Then $|\mathrm{Aut}(S)|$ is at most $1\,045\,094\,400$ and $|\mathrm{Aut}(S)||\mathrm{Out}(S)|$ is at most $6\,270\,566\,400$.

Proof. The possibilities for S come from Theorem 6.2.10. The order of ${}^2\mathrm{E}_6(3)$ is $2^{19}.3^{36}.5^2.7^3.13.19.37.41.61.73$. Then we may rule out those subgroups S whose order does not divide $|{}^2\mathrm{E}_6(3)|$, and those in characteristic 3. Then we are left with those subgroups given above. We see that both $|\mathrm{Aut}(S)|$ and $|\mathrm{Aut}(S)||\mathrm{Out}(S)|$ are largest when $S = \mathrm{P}\Omega_8^+(2)$. □

Lemma 6.3.37. *Let S be a simple subgroup of ${}^2\mathrm{E}_6(3)$, where S is of Lie type in characteristic 2 such that $\mathrm{rk}(S) \leq 3$. Then S is isomorphic to one of the following:*

$$\begin{array}{l} \mathrm{PSL}_2(3^k) \text{ for } k \leq 5, \\ \mathrm{PSL}_3(3^k) \text{ for } k \leq 2, \\ \mathrm{PSL}_4(3^k) \text{ for } k \leq 2, \\ \mathrm{PSU}_3(3^k) \text{ for } k \leq 2, \\ \mathrm{PSp}_4(3^k) \text{ for } k \leq 2, \\ \mathrm{G}_2(3^k) \text{ for } k \leq 2, \\ \mathrm{PSU}_4(3), \mathrm{PSp}_6(3), \Omega_7(3), {}^2\mathrm{G}_2(27), \mathrm{P}\Omega_8^-(3), \end{array}$$

and $|\mathrm{Aut}(S)||\mathrm{Out}(S)| \leq 12\,994\,519\,832\,985\,600$.

Proof. Possibilities for S come from Theorem 6.3.8. Theorem 6.2.9 bounds the order of maximal subgroups M with socle S, and therefore bounds the order of subgroups S. The order of ${}^2\mathrm{E}_6(3)$ is $2^{19}.3^{36}.5^2.7^3.13.19.37.41.61.73$. Then we rule out the subgroups whose order does not divide $|{}^2\mathrm{E}_6(3)|$ and we are left with the possibilities listed above. We see that $|\mathrm{Aut}(S)||\mathrm{Out}(S)|$ is largest when $S = \mathrm{PSL}_4(9)$. □

Lemma 6.3.38. *Let G be an almost simple group with socle ${}^2\mathrm{E}_6(3)$. Then*

$$\sum_{M\in\mathcal{U}} \frac{1}{[G:M]^2} \leq \frac{2050}{34587}.$$

Proof. Possibilities for $S \in \mathcal{S}$ come from Lemma 6.3.36 and Lemma 6.3.37. We use Lemma 3.2.12 taking $c = |\mathrm{Aut}(\mathrm{PSL}_4(9))||\mathrm{Out}(\mathrm{PSL}_4(9))|$ as an upper bound for the order of $M \in \mathcal{U}$. For an involution t in a conjugacy class of maximal size we use $|C_{2\mathrm{E}_6(3)}(t)| = |\mathrm{SL}_2(3)||\mathrm{SL}_6(3)|$ from Table 6.6 and we estimate $i({}^2\mathrm{E}_6(3)) \leq 5[G : C_{2\mathrm{E}_6(3)}(t)]$. Then,

$$\begin{aligned}\sum_{M\in\mathcal{U}} \frac{1}{[G:M]^2} &\leq \frac{i({}^2\mathrm{E}_6(3))c}{|{}^2\mathrm{E}_6(3)|} \\ &\leq \frac{5c}{|\mathrm{SL}_2(3)||\mathrm{SU}_6(3)|} \\ &= \frac{2050}{34587}.\end{aligned}$$

□

Then, we may bound the probability.

Lemma 6.3.39. *Let G be an almost simple group with socle ${}^2\mathrm{E}_6(3)$. Then $P_{G,{}^2\mathrm{E}_6(3)}(2) > 0.940$.*

Proof. Lemma 6.2.8 bounds $\sum_{M\in\mathcal{K}} 1/[G:M]^2$, and Lemma 6.3.34 bounds $\sum_{M\in\mathcal{U}} 1/[G:M]^2$. Then by Lemma 3.2.6,

$$P_{G,E_6(3)}(2) \geq 1 - (\sum_{M\in\mathcal{K}} \frac{1}{[G:M]^2} + \sum_{M\in\mathcal{U}} \frac{1}{[G:M]^2}) > 0.940.$$

□

We may combine all the results for $\mathrm{F}_4(q)$, $\mathrm{E}_6(q)$ and ${}^2\mathrm{E}_6(q)$.

Theorem 6.3.40. *Let G be an almost simple group with socle $\mathrm{F}_4(q)$. Then $P_{G,\mathrm{F}_4(q)}(2) > 0.947$.*

Proof. For $q \geq 19$, this comes from Theorem 6.3.1. For odd primes q, $\mathrm{Out}(\mathrm{F}_4(q)) = 1$, and so for odd primes $q \geq 5$, $P_{G,\mathrm{F}_4(q)}(2) = P_{\mathrm{F}_4(q)} > 0.999$ by Theorem 6.3.7. Then it remains to estimate the probability for $q = 2, 3, 4, 8, 9, 16$. Probability estimates for all of these but $q \neq 2$ come from Lemmas 6.3.15, 6.3.19, 6.3.23, 6.3.27 and 6.3.31. Finally when $q = 2$, $G = \mathrm{F}_4(2)$ or $\mathrm{Aut}(\mathrm{F}_4(2))$. In both these cases the maximal subgroups are known and given in the Atlas ([39] states that these lists of maximal subgroups are complete). By Lemma 3.2.6, $P_{G,\mathrm{F}_4(2)}(2) > 0.999$ completing the proof. □

Theorem 6.3.41. *Let G be an almost simple group with socle $\mathrm{E}_6(q)$. Then $P_{G,\mathrm{E}_6(q)}(2) > 0.935$.*

Proof. By Theorem 6.3.2, if $q \geq 4$, then $P_{G,\mathrm{E}_6(q)}(2) > 0.993$. By Lemma 6.3.35, $P_{G,\mathrm{E}_6(3)}(2) > 0.935$. Finally if $q = 2$ then $G = \mathrm{E}_6(2)$ or $\mathrm{Aut}(\mathrm{E}_6(2))$. In both these cases the maximal subgroups are known [45] and so we may calculate $P_{G,\mathrm{E}_6(2)}(2) > 0.999$. □

Theorem 6.3.42. *Let G be an almost simple group with socle ${}^2\mathrm{E}_6(q)$. Then $P_{G,{}^2\mathrm{E}_6(q)}(2) > 0.940$.*

Proof. By Theorem 6.3.3, if $q \geq 4$, then $P_{G,{}^2\mathrm{E}_6(q)}(2) > 0.993$. By Lemma 6.3.39, $P_{G,{}^2\mathrm{E}_6(q)}(2) > 0.940$. Finally if $q = 2$ then $G = G_0$, $G_0.2$, $G_0.3$, or $G_0.S_3$. In all these cases the maximal subgroups are known (given in the Atlas [17], [39], [94]) and so we calculate $P_{G,{}^2\mathrm{E}_6(2)}(2) > 0.999$ □

Now we can complete the proof of the main theorem of this chapter and bound $P_{G,G_0}(2)$ below for the exceptional groups.

Proof of Theorem 6.0.1. If G_0 is one of ${}^2\mathrm{B}_2(q)$, $\mathrm{G}_2(q)$, ${}^2\mathrm{G}_2(q)$, ${}^3\mathrm{D}_4(q)$, ${}^2\mathrm{F}_4(q)$ or ${}^2\mathrm{F}_4(2)'$ then by Theorem 6.1.16, $P_{G,G_0}(2) > 0.931$. The remaining possibilities for G_0 are $\mathrm{F}_4(q)$, $\mathrm{E}_6(q)$, ${}^2\mathrm{E}_6(q)$, $\mathrm{E}_7(q)$, or $\mathrm{E}_8(q)$. If $G_0 = \mathrm{E}_7(q)$ or $\mathrm{E}_8(q)$, then $P_{G,G_0}(2) > 0.999$ by Theorems 6.3.4 and 6.3.5. Finally if G_0 is $\mathrm{F}_4(q)$, $\mathrm{E}_6(q)$, or ${}^2\mathrm{E}_6(q)$, then $P_{G,G_0}(2) > 0.935$ by Theorems 6.3.40, 6.3.41 and 6.3.42. □

Chapter 7

The probability of generating a sporadic group

In this chapter we prove the following theorem which bounds $P_{G,G_0}(2)$ for almost simple groups G with socle G_0 a sporadic group. This, together with Theorems 4.0.1, 5.0.1 and 6.0.1, concludes the proof of Theorem 3.1.7 and bounds $P_{G,G_0}(2)$ for almost simple groups G with socle G_0.

Theorem 7.0.1. *Let G be an almost simple group with socle G_0, where G_0 is a sporadic group. Then $P_{G,G_0}(2) > 0.813$ and if $G \neq M_{11}, M_{12}$ then $P_{G,G_0}(2) > 0.930$.*

Proof. This is proved for all groups other than the Monster in Lemma 7.1.1 and Theorem 7.2.5 proves this for the Monster. □

Maximal subgroups of all sporadic groups other than the Monster are known, and so we consider these first. Once again, we round all decimal values of probabilities down to three decimal places.

7.1 Sporadic groups other than the Monster

Lemma 7.1.1. *Let G be an almost simple group with socle G_0, where G_0 is a sporadic group other than the Monster. Then $P_{G,G_0}(2) > 0.813$, and $P_{G,G_0}(2) \leq 0.930$ if and only if $G = \mathrm{M}_{11}$ or M_{12}.*

Proof. There are 12 sporadic groups with outer automorphism groups of order 2: M_{12}, M_{22}, J_2, J_3, HS, Suz, McL, He, O′N, Fi_{22}, Fi'_{24}, HN. All other sporadic groups have trivial outer automorphism groups. Then in all cases $G = G_0$ or $G = \mathrm{Aut}(G_0)$. For smaller sporadic groups (those whose table of marks is available in GAP [28]), we can calculate the exact probability $P_{G,G_0}(2)$ in the case where $G = G_0$. These values are displayed in Table 7.1. For some of these groups we have also calculated exact values for the probability in the case where $G = \mathrm{Aut}(G_0)$ and these values are listed in

Table 7.2. For the remaining sporadic groups there are complete lists of maximal subgroups of G_0 and $\mathrm{Aut}(G_0)$ in the Online Atlas [94], and so we calculate a lower bound for the probability using Lemma 3.2.6. These lower bounds are listed in Tables 7.3 and 7.4. Then it is clear that for all almost simple groups G with socle a sporadic group other than the Monster, $P_{G,G_0}(2) > 0.813$, and $P_{G,G_0}(2) \leq 0.930$ if and only if $G = \mathrm{M}_{11}$ or M_{12} (if $G = \mathrm{M}_{22}$, then $P_{G,G_0}(2) > 0.930$). □

$\lvert G\rvert$	G	$P_G(2)$	$P_G(2)$
7 920	M_{11}	3239/3960	0.817
95 040	M_{12}	179/220	0.813
175 560	J_1	14541/14630	0.993
443 520	M_{22}	9377/10080	0.930
604 800	J_2	296579/302400	0.980
1 020 0960	M_{23}	1210247/1275120	0.949
44 352 000	HS	4377/4480	0.977
50 232 960	J_3	25103957/25116480	0.999
244 823 040	M_{24}	2779979/2914560	0.953
898 128 000	McL	55857449/56133000	0.995
4 030 387 200	He	2013860879/2015193600	0.999
495 766 656 000	Co_3	61737820351/61970832000	0.996

Table 7.1: Exact probabilities for small sporadic groups G

G	G_0	$P_{G,G_0}(2)$	$P_{G,G_0}(2)$
$\mathrm{M}_{12}.2$	M_{12}	7763/7920	0.980
$\mathrm{M}_{22}.2$	M_{22}	26011/27720	0.938
$\mathrm{J}_2.2$	J_2	296591/302400	0.980
$\mathrm{J}_3.2$	J_3	1673809/1674432	0.999
McL.2	McL	55912337/56133000	0.996
HS.2	HS	10956917/11088000	0.988
He.2	He	2013937111/2015193600	0.999

Table 7.2: Exact conditional probabilities for small almost simple groups $G = \mathrm{Aut}(G_0)$

7.2 The probability of generating the Monster

Now let $G_0 = \mathrm{M}$. Recall $\mathrm{Out}(\mathrm{M}) = 1$, and so if G is an almost simple group with socle G_0, then $G = G_0$. Let $\mathcal{L}$ be a set of conjugacy class representatives for maximal subgroups of M.

$\lvert G_0\rvert$	G_0	$P_{G_0}(2) \geq$
145 926 144 000	Ru	0.999
448 345 497 600	Suz	0.999
460 815 505 920	O′N	0.999
42 305 421 312 000	Co_2	0.999
64 561 751 654 400	Fi_{22}	0.999
273 030 912 000 000	HN	0.999
51 765 179 004 000 000	Ly	0.999
90 745 943 887 872 000	Th	0.999
4 089 470 473 293 004 800	Fi_{23}	0.999
4 157 776 806 543 360 000	Co_1	0.999
86 775 571 046 077 562 880	J_4	0.999
1 255 205 709 190 661 721 292 800	Fi'_{24}	0.999
4 154 781 481 226 426 191 177 580 544 000 000	B	0.999

Table 7.3: Lower bounds for $P_{G_0}(2)$ for some sporadic groups G_0

G	G_0	$P_{G,G_0}(2) \geq$
Suz.2	Suz	0.999
O′N.2	O′N	0.999
$Fi_{22}.2$	Fi_{22}	0.999
Fi_{24}	Fi'_{24}	0.999
HN.2	HN	0.999

Table 7.4: Lower bounds for $P_{G,G_0}(2)$ for some almost simple groups $G = \mathrm{Aut}(G_0)$

Again, we will estimate the probability of generating the Monster by estimating the number and order of maximal subgroups. Whilst the maximal subgroups of the Monster have not been determined completely, we have enough information to estimate the sum.

Recall a subgroup H of a group G is *p-local* if it is the normaliser of a p-subgroup of G.

Lemma 7.2.1. *Let G be a finite non-abelian simple group and let L be a maximal subgroup of G. Then L is a p-local group, the normaliser of a direct product of 2 or more non-abelian simple groups, or it is almost simple.*

Proof. Let K be a minimal normal subgroup of L. Then K is the direct product of isomorphic simple groups. As G is almost simple, $L = N_G(K)$. If K is the direct product of isomorphic cyclic groups C_p then it is a p-group, and so L is p-local. If K is a non-abelian almost simple group then L is almost simple. The remaining possibility is that K is the direct product of

more than one non-abelian simple group and the result follows. □

So we can split the maximal subgroups of the Monster into these three cases.

Lemma 7.2.2. *Let $\mathcal{L}_1$ be a set of conjugacy class representatives for maximal subgroups of* M *which are p-local subgroups. Then*

$$\sum_{L\in\mathcal{L}_1} \frac{1}{[\mathrm{M} : L]} \leq \frac{39}{10^{18}}.$$

Proof. The subgroups which are maximal amongst the p-local subgroups of the Monster are known up to conjugacy. Note that these subgroups may or may not be maximal in M. When $p = 2$ these subgroups are listed in [72] (in fact, this paper confirms that the list of maximal 2-local subgroups of the Monster given in the Atlas is complete). There are 7 such subgroups up to conjugacy, each of index greater than 10^{18}. When $p \geq 3$, the subgroups which are maximal amongst the p-local subgroups are given in [91]. There are 32 such subgroups up to conjugacy, each of index greater than 10^{18}. The result follows. □

Lemma 7.2.3. *Let $\mathcal{L}_2$ be the set of $L \in \mathcal{L}$ such that L is the normaliser of two or more simple groups. Then*

$$\sum_{L\in\mathcal{L}_2} \frac{1}{[\mathrm{M} : L]} \leq \frac{9}{10^{30}}.$$

Proof. Maximal subgroups which are normalisers of products of 2 or more simple groups are listed in the Atlas. This list is complete as stated in the 'Improvements to the Atlas' (available from the Online Atlas [94]). There are 9 such maximal subgroups up to conjugacy, each of which has index greater than 10^{30}. The result follows. □

Finally, we consider almost simple maximal subgroups of M.

Lemma 7.2.4. *Let $\mathcal{L}_3$ be the set of $L \in \mathcal{L}$ such that L is an almost simple group. Then*

$$\sum_{L\in\mathcal{L}_3} \frac{1}{[M : L]} \leq 0.000000704.$$

Proof. Let $\mathcal{K}$ be the set of all almost simple maximal subgroups of M. As M is a simple group,

$$\sum_{L\in\mathcal{L}_3} \frac{1}{[\mathrm{M} : L]} = \sum_{L\in\mathcal{K}} \frac{1}{[\mathrm{M} : L]^2}.$$

Norton and Wilson [77] list all possible simple subgroups of the Monster (the subgroup $\mathrm{PSL}_2(41)$ was missing from this list [93]). The largest

possible almost simple maximal subgroup has order $|\mathrm{Aut}(\mathrm{Fi}_{23})| = |\mathrm{Fi}_{23}| = 4\,089\,470\,473\,293\,004\,800$ and the largest outer automorphism group for any possible simple subgroup S is $|\mathrm{Out}(S)| = 24$ (corresponding to $S = \mathrm{P}\Omega_8^+(3)$). We shall use the fact that for an almost simple group L with socle S, we may bound the order by $|L| \leq |S||\mathrm{Out}(S)|$ and so $|L| \leq 24|S|$. Let $\mathcal{S}(\mathrm{M})$ denote the set of non-abelian simple subgroups of M. Then, using Lemma 3.2.12

$$\begin{aligned}
\sum_{L\in\mathcal{K}} \frac{1}{[\mathrm{M}:L]^2} &= \sum_{L\in\mathcal{K}} \frac{|L|^2}{|\mathrm{M}|^2} \\
&\leq \frac{|\mathrm{Fi}_{23}|}{|\mathrm{M}|^2} \sum_{L\in\mathcal{K}} |L| \\
&\leq \frac{4\,089\,470\,473\,293\,004\,800}{|\mathrm{M}|^2} \sum_{S\in\mathcal{S}(\mathrm{M})} 24|S| \\
&\leq \frac{24\times 4\,089\,470\,473\,293\,004\,800}{|\mathrm{M}|^2} \sum_{S\in\mathcal{S}(\mathrm{M})} |S| \\
&\leq \frac{24\times 4\,089\,470\,473\,293\,004\,800}{|M|^2} \times |M|i(M).
\end{aligned}$$

Now, the Atlas tells us that there are two conjugacy classes of involutions in the Monster. The number of conjugates of an element $t \in \mathrm{M}$ is given by $[\mathrm{M} : C_{\mathrm{M}}(t)]$. As the orders of centralisers of conjugacy class representatives are listed in the Atlas we may calculate the number of involutions. We obtain $i(\mathrm{M}) = 5\,791\,748\,165\,751\,443\,778\,953\,445\,375$ and so,

$$\sum_{L\in\mathcal{L}_3} \frac{1}{[\mathrm{M}:L]} \leq 0.000000704.$$

□

Combining these results we have the following.

Theorem 7.2.5. *The probability of generating the Monster with two elements is greater than* 0.999.

Proof. Lemmas 7.2.2, 7.2.3, 7.2.4 give

$$\sum_{L\in\mathcal{L}} \frac{1}{[\mathrm{M}:L]} < 7.05\times 10^{-7}.$$

Then

$$P_{\mathrm{M}}(2) > 0.999.$$

□

This, together with Lemma 7.1.1, concludes the proof of Theorem 7.0.1.

Chapter 8

The probability of generating an almost simple group with 3 elements

Recall that an almost simple group G can be generated by 3 elements (Theorem 3.1.6). In this chapter we prove the following.

Theorem 8.0.1. *Let G be an almost simple group with socle G_0. Then $P_{G,G_0}(3) \geq 139/150 = 0.92\dot{6}$, with equality if and only if $G_0 = A_5$.*

Let $\mathcal{M}$ be a set of conjugacy class representatives for maximal subgroups of G not containing G_0. Then the previous chapters bound $P_{G,G_0}(2)$ using variants of Lemma 3.2.6 and estimating $\sum_{M\in\mathcal{M}} 1/[G : M]$. It would be easy to modify these bounds to bound $\sum_{M\in\mathcal{M}} 1/[G : M]^2$ and hence bound $P_{G,G_0}(3)$ below. To reduce the need for much further calculation we observe that if G can be generated by 3 elements then $P_{G,G_0}(3) \geq P_{G,G_0}(2)$ (Lemma 3.2.13). By Theorem 3.1.6, if G is an almost simple group with socle G_0, then we have the following possibilities:

1. G can be generated by 2 elements;
2. $G_0 = \mathrm{PSL}_n(p^f)$ for $n \geq 4$ even, $p \geq 3$ and $f \geq 2$ even;
3. $G_0 = \mathrm{P}\Omega_n^+(p^f)$ for $n \geq 8$, $p \geq 3$ and $f \geq 2$ even.

First we consider the case where G can be generated by two elements, and we combine previous estimates for the probability of 2-generation and Lemma 3.2.13. We shall estimate $P_{G,G_0}(3)$ for 3-generated almost simple groups using Lemma 3.2.6 in a similar way to our estimates for $P_{G,G_0}(2)$.

From previous chapters we see that $P_{G,G_0}(2) \geq 0.927$ except for finitely many almost simple groups G. We summarise these results as follows.

Lemma 8.0.2. *Let G be an almost simple group with socle G_0 and suppose G can be generated by two elements. If $P_{G,G_0}(2) < 0.927$ then one of the following holds.*

1. *G_0 is an alternating group of degree at most 16.*
2. *G is isomorphic to M_{11} or M_{12}.*
3. *G_0 is isomorphic to one of $\mathrm{PSL}_2(7)$, $\mathrm{PSL}_2(8)$, $\mathrm{PSL}_2(11)$, $\mathrm{PSL}_2(13)$, $\mathrm{PSL}_2(16)$, $\mathrm{PSU}_3(3)$, $\mathrm{PSp}_4(3)$ or $\mathrm{PSp}_6(2)$.*
4. *G is isomorphic to one of $\mathrm{PSL}_2(17)$, $\mathrm{PSL}_2(19)$, $\mathrm{PSL}_3(3)$, $\mathrm{PSL}_3(4)$, $\mathrm{PGL}_3(4)$, $\mathrm{PSL}_3(4).2_1$, $\mathrm{PSL}_3(4).2_2$ or $\mathrm{P\Gamma L}_3(4)$.*

Proof. This follows from Lemma 4.9.2 and Theorems 5.0.1, 6.0.1 and 7.0.1. □

Then if G can be generated by two elements $P_{G,G_0}(3) \geq P_{G,G_0}(2) \geq 0.927$, except possibly in the cases in the previous lemma. The probability $P_{G,G_0}(3)$ (or at least a lower bound) for these groups can be calculated computationally. Exact values for $G_0 = A_n$ for $n \leq 13$, $G = M_{11}$ and $G = M_{12}$ have been calculated using GAP [28] and these values are displayed in Table 8.1. For slightly larger n we may obtain maximal subgroups of A_n and S_n in GAP [28], and therefore we obtain a lower bound on the probability (lower bounds are given in Table 8.2). For the classical groups we calculate a lower bound for the probability using the `ClassicalMaximals` function in Magma [8], and these results are shown in Table 8.3.

Now suppose that G is almost simple and $d(G) = 3$. Then $G_0 = \mathrm{PSL}_n(p^f)$ for $n \geq 4$ even, $p \geq 3$ and $f \geq 2$ even; or $G_0 = \mathrm{P\Omega}_n^+(p^f)$ for $n \geq 8$, $p \geq 3$ and f even.

Lemma 8.0.3. *Let G be an almost simple group with socle G_0.*

1. *If $G_0 = \mathrm{PSL}_n(q)$ for $n \geq 4$ and $q \geq 9$ then*

$$P_{G,G_0}(3) \geq 1 - \frac{(2n^{5.2} + n\log\log q)(q-1)^2}{(q^n-1)^2}$$

   and $P_{G,G_0}(3) \geq 0.995$.

2. *If $G_0 = \mathrm{P\Omega}_n^+(q)$ for $n \geq 8$ and $q \geq 9$ then*

$$P_{G,G_0}(3) \geq 1 - \frac{(2n^{5.2} + n\log\log q)(q-1)^2}{(q^{n/2}-1)^2(q^{n/2-1}+1)^2}$$

   and $P_{G,G_0}(3) \geq 0.999$.

G	G_0	$P_{G,G_0}(3)$	$P_{G,G_0}(3)$
A_5	A_5	139/150	0.926
S_5	A_5	139/150	0.926
A_6	A_6	93/100	0.930
S_6	A_6	93/100	0.930
$\mathrm{PGL}_2(9)$	A_6	89/90	0.988
M_{10}	A_6	89/90	0.988
$A_6.2^2$	A_6	89/90	0.988
A_7	A_7	51269/52920	0.968
S_7	A_7	1759/1800	0.977
A_8	A_8	1832591/1881600	0.973
S_8	A_8	16633523/16934400	0.982
A_9	A_9	270705163/274337280	0.986
S_9	A_9	193387661/195955200	0.986
A_{10}	A_{10}	135727194541/137168640000	0.989
S_{10}	A_{10}	135727194541/137168640000	0.989
A_{11}	A_{11}	1371285452279/1383117120000	0.991
S_{11}	A_{11}	2742571768091/2766234240000	0.991
A_{12}	A_{12}	790984643190757/796675461120000	0.992
S_{12}	A_{12}	12555315748807/12645642240000	0.992
A_{13}	A_{13}	401469630747973993/403914458787840000	0.993
S_{13}	A_{13}	10294093096168517/10356780994560000	0.993
M_{11}	M_{11}	233897/237600	0.984
M_{12}	M_{12}	185492987/188179200	0.985

Table 8.1: $P_{G,G_0}(3)$ for almost simple groups G with socle G_0

n	$P_{A_n}(3) \geq$	$P_{S_n,A_n}(3) \geq$
14	0.994	0.994
15	0.995	0.995
16	0.996	0.996

Table 8.2: Lower bounds on $P_{G,A_n}(3)$ for $G = S_n$ or A_n

G_0	$P_{G,G_0}(3) \geq$	G_0	$P_{G,G_0}(3) \geq$
$\mathrm{PSL}_2(7)$	0.940	$\mathrm{PSL}_2(19)$	0.996
$\mathrm{PSL}_2(8)$	0.985	$\mathrm{PSL}_3(3)$	0.987
$\mathrm{PSL}_2(11)$	0.975	$\mathrm{PSL}_3(4)$	0.994
$\mathrm{PSL}_2(13)$	0.994	$\mathrm{PSU}_3(3)$	0.997
$\mathrm{PSL}_2(16)$	0.996	$\mathrm{PSp}_4(3)$	0.996
$\mathrm{PSL}_2(17)$	0.996	$\mathrm{PSp}_6(2)$	0.997

Table 8.3: Lower bounds for $P_{G,G_0}(3)$ for any almost simple group G with socle G_0

Proof. Let $\mathcal{M}$ be a set of conjugacy class representatives for maximal subgroups of G not containing G_0. By Lemma 3.2.6,

$$P_{G,G_0}(3) \geq 1 - \sum_{M \in \mathcal{M}} \frac{1}{[G:M]^2}.$$

The index $[G:M]$ may be bounded below by the minimal index of a subgroup in G_0, which is equal to $\rho(G_0)$, the minimal degree of a permutation representation of G_0. The number of conjugacy classes of maximal subgroups of G not containing G_0 is denoted $m(G)$. Then

$$P_{G,G_0}(3) \geq 1 - \frac{m(G)}{\rho(G_0)^2}.$$

The values for $m(G)$ and $\rho(G_0)$ come from Theorem 5.1.1 and Theorem 2.2.42. These estimates are increasing with increasing n and q, and so we get the lower bounds given. □

Now we bound $P_{G,G_0}(3)$ below, hence proving Theorem 3.1.8.

Proof of Theorem 3.1.8. Theorem 3.1.6 shows that either $d(G) = 2$, or $d(G) = 3$ and $G_0 = \mathrm{PSL}_n(q)$ or $\mathrm{P}\Omega_n^+(q)$ as in Lemma 8.0.3.

First suppose $d(G) = 2$. By Lemma 3.2.13, $P_{G,G_0}(3) \geq P_{G,G_0}(2)$. Then by Lemmas 8.0.2, and computational results from Tables 8.1, 8.2 and 8.3, $P_{G,G_0}(3) \geq 139/150 = 0.92\dot{6}$ with equality if and only if $G_0 = A_5$.

Next suppose $d(G) = 3$. Then $G_0 = \mathrm{PSL}_n(q)$, with $n \geq 4$ and $q \geq 9$, or $G_0 = \mathrm{P}\Omega_n^+(q)$ with $n \geq 8$ and $q \geq 9$. By Lemma 8.0.3, $P_{G,G_0}(3) \geq 0.995$, completing the proof. □

Part II

Random generation and chief length of finite groups

Chapter 9

Random generation and chief length of finite groups

In the second part of this thesis we continue to study random generation, but in this case we are given a failure probability ϵ, and wish to estimate $d^\epsilon(G)$, the number of random elements required to generate G with failure probability at most ϵ. A modification of a result of Lubotzky [64] bounds this number in terms of the minimal number of generators for G, and the chief length of G. We seek to use these bounds when G is a permutation group or a matrix group, and we concentrate on improving bounds on the chief length in these cases.

First we give some basic definitions for the chief length and some preliminary lemmas, before discussing results on the number of random elements required to generate a group G. The following two chapters bound the chief length of permutation groups in terms of the degree n, and the chief length of matrix groups in terms of the dimension n and the field size q. In both these cases we see how these bounds, together with existing bounds on the number of generators of G, give a tighter bound on $d^\epsilon(G)$ for permutation or matrix groups.

9.1 Chief series and chief length

Definition 9.1.1. A *subnormal series* for a group G is a finite chain of subgroups $1 = G_0 < G_1 < \ldots < G_n = G$, such that G_i is a normal subgroup of G_{i+1} for $i = 0, \ldots, n-1$. The quotient groups G_{i+1}/G_i are the *factors* and n is the *length* of the series.

Recall that H is a *subnormal* subgroup of G, denoted $H \lhd\lhd G$, if there exists a series $H = H_0 < H_1 < \ldots < H_n = G$, in which H_i is normal in H_{i+1}.

Definition 9.1.2. A series $H_0 < H_1 < \ldots < H_m = G$ is a *refinement* of

the series $1 = G_0 < G_1 < \ldots < G_n = G$ if there are integers $0 \leq j_0 < j_1 < \ldots < j_n \leq m$ such that $G_i = H_{j_i}$ for $i = 0, 1, \ldots, n$.

Definition 9.1.3. A subnormal series in which all the factors are simple is called a *composition series* and its factors are called *composition factors*.

Thus a composition series is a subnormal series which cannot be further refined.

Theorem 9.1.4 (Jordan–Hölder)**.** *Let $1 = G_0 < \ldots < G_n = G$ and $1 = H_0 < \ldots < H_m = G$ be two composition series for a group G. Then $n = m$ and there is a one-to-one correspondence between the two multisets of composition factors such that the corresponding factors are isomorphic.*

A proof of this is given in [83, Theorem 7.9]. In particular, this shows that all composition series of a group G have the same length, allowing us to make the following definition.

Definition 9.1.5. The *composition length* of a group G is the length of a composition series of G. We denote the composition length of G by $c(G)$.

Definition 9.1.6. A *normal series* is a series $1 = G_0 < G_1 < \ldots < G_n = G$ in which each subgroup G_i is normal in G.

Definition 9.1.7. A *chief series* for G is a normal series $1 = N_0 \lhd N_1 \lhd \ldots \lhd N_l = G$ in which N_{i+1}/N_i is minimal normal in G/N_i for $i = 0, \ldots, l-1$. The quotient groups N_{i+1}/N_i are the *chief factors*.

That is, a chief series for G is a normal series for G which cannot be further refined to another normal series. An argument similar to the proof of the Jordan–Hölder Theorem tells us that any two chief series of G have the same length, and the chief factors are the same.

Lemma 9.1.8. *Any normal series for G may be refined to a chief series for G. In particular, any group G has a chief series.*

Proof. Let $1 = H_0 < H_1 < \ldots < H_n = G$ be a normal series for G. If this is not a chief series for G, then H_{i+1}/H_i is not a minimal normal subgroup of G/H_i for some i. Then we may pick a minimal normal subgroup K/H_i of G/H_i such that $K/H_i \leq H_{i+1}/H_i$. Then K is a normal subgroup of G, and we have refined our normal series to $1 = H_0 < \ldots < H_i < K < H_{i+1} < \ldots < G$. We keep refining our series in this way until all consecutive terms K_i, K_{i+1} are such that K_{i+1}/K_i is minimal normal in G/K_i, that is, we have a chief series for G (this process of refinement terminates as we are dealing with finite groups).

It follows that if we are given any group G, then the normal series $1 \leq G$ may be refined to a chief series. □

Lemma 9.1.9. *Let K be a minimal normal subgroup of a group G. Then K is characteristically simple.*

Proof. Let N be a proper characteristic subgroup of K. As K is normal in G, conjugation by $g \in G$ induces an automorphism of K. Then as N is characteristic, $N^g = N$ for all $g \in G$, that is, N is normal in G. Then N must be trivial otherwise it would contradict the minimality of K. Then K is characteristically simple. □

In particular, this shows that all chief factors are characteristically simple and so are the direct product of isomorphic simple groups.

Lemma 9.1.10. *Let $N \trianglelefteq G$. Then there exists a chief series $1 = G_0 < G_1 < \ldots < G_n = G$ where $N = G_i$ for some $1 \leq i \leq n$.*

Proof. The series $1 \leq N \leq G$ is a normal series for G, and by Lemma 9.1.8, this may be refined to a chief series for G. □

Definition 9.1.11. The *chief length* of a group G is the length of a chief series of G. We denote the length of a chief series by $l(G)$. If N is a normal subgroup of G, the length of the part of the chief series from 1 to N will be denoted $l_G(N)$.

Note that $l_G(G) = l(G)$. As a chief series may be refined to be a composition series, the chief length is bounded above by the composition length. We have a basic bound for the length of any series of G given by $\log |G|$, as each factor group has order at least 2. This bound is achieved for the chief length precisely when G is a 2-group. This is an example of the following.

Lemma 9.1.12. *Let $|G| = p^n$. Then for $0 \leq i \leq n$, G has a normal subgroup N_i of order p^i such that $1 = N_0 < N_1 < \ldots < N_n = G$.*

Proof. We shall prove this by induction. This theorem holds when $n = 1$, and we shall assume that it is true for any group of order p^{n-1} for some $n > 1$. If G is a group of order p^n, as it is a p-group, the centre is non-trivial. We may choose a non-identity element $a \in Z(G)$, whose order is some power of p. By taking an appropriate power of a we find an element x of order p in $Z(G)$. Then $N_1 = \langle x \rangle$ is a normal subgroup of $Z(G)$ of order p. Let $\bar{G} = G/N_1$, a group of order p^{n-1}. By the induction hypothesis it has normal subgroups $\bar{N}_1 < \bar{N}_2 < \ldots < \bar{N}_n = \bar{G}$ (where $\bar{N}_i$ has order p^{i-1}). By the Correspondence Theorem, $\bar{N}_i = N_i/N_1$ where $N_1 \lhd N_i \lhd G$. Then $1 = N_0 < N_1 < \ldots < N_n$ is a sequence of normal subgroups with the required properties. □

Note that $1 = N_0 < N_1 < \ldots < N_n = G$ is a chief series for G and so we obtain the following corollary.

Corollary 9.1.13. *If G is a p-group, then $l(G) = \log_p |G|$.*

We prove other basic facts about the chief length.

Lemma 9.1.14. *Let $H \trianglelefteq K \trianglelefteq G$ where $H \trianglelefteq G$. Then $l_G(H) \leq l_K(H)$.*

Proof. The normal series $1 \trianglelefteq H \trianglelefteq K \trianglelefteq G$ may be refined to a chief series for G,

$$1 = N_0 \trianglelefteq \ldots \trianglelefteq N_i = H \trianglelefteq N_{i+1} \trianglelefteq \ldots \trianglelefteq N_j = K \trianglelefteq N_{j+1} \trianglelefteq \ldots \trianglelefteq N_l = G.$$

This is a chief series which passes through both H and K, and where $l_G(H) = i$. Then the normal series

$$1 = N_0 \trianglelefteq \ldots \trianglelefteq N_i = H \trianglelefteq N_{i+1} \trianglelefteq \ldots \trianglelefteq N_j = K,$$

may be refined to a chief series for K, and thus $l_K(H) \geq i = l_G(H)$ as required. □

If $K = H$ this implies that $l_G(H) \leq l(H)$.

Lemma 9.1.15. *Let $N \trianglelefteq G$. Then $l(G) = l_G(N) + l(G/N)$. In particular, $l(G) \leq l(N) + l(G/N)$.*

Proof. Let $1 = M_0 < \ldots < M_k = N < M_{k+1} < \ldots < M_t = G$ be a chief series for G passing through N. Then $l_G(N) = k$ and $l(G) = t$. For $k \leq i \leq t$, M_i/N is a normal subgroup of G/N, and $M_k/N < M_{k+1}/N < \ldots < G/N$ is a normal series for G/N. The minimality of N_{i+1}/N_i in G/N_i gives the minimality of $\frac{N_{i+1}/N}{N_i/N} \cong N_{i+1}/N_i$ in $\frac{G/N}{N_i/N} \cong G/N_i$ and so this is a chief series for G/N. Then $l(G/N) = t - k$, and so the theorem holds. □

In some cases we may have equality for $l(G) \leq l(N) + l(G/N)$, for example, if G is a p-group, if N is a simple group, or if $N = Z(G)$. Equality does not always hold: consider the case when $G = S_4$ and N is the Klein four group (the minimal normal subgroup of S_4). Then $l(G) = 3$ but $l(N) = 2$ and $l(G/N) = 2$.

Lemma 9.1.16. *Suppose $G = H \times K$. Then $l(G) = l(H) + l(K)$.*

Proof. This follows as a subgroup is normal in H if and only if it is normal in $H \times K$. □

It will be useful to have results for subdirect products, not just direct products.

Lemma 9.1.17. *Let G be a subdirect product of H and K. Then $l(G) \leq l(H) + l(K)$ with equality if and only if $G = H \times K$.*

Proof. Let π_1 be a projection map from G onto H, and let π_2 be a projection map from G onto K. Then $N = \ker \pi_1 \leq 1 \times K \cong K$ is a normal subgroup of G. As G is a subdirect product, $\operatorname{im} \pi_1 = H$, and so by the First Isomorphism Theorem, $G/N \cong H$. Then, by Lemma 9.1.15, $l(G) = l_G(N) + l(H)$. Thus, we wish to show that $l_G(N) \leq l(K)$.

Consider a subgroup $L \trianglelefteq G$ such that $L \leq 1 \times K$. Then let $J = L\pi_2$. As $L \leq 1 \times K$, it follows that $J \cong L$. We show that J is normal in K. Choose $l \in J$ and $k \in K$. Then there exists some $(1, l) \in L$, and some $h \in H$ such that $(h, k) \in G$. As L is normal in G, $(h, k)^{-1}(1, l)(h, k) = (1, k^{-1}lk) \in L$. So $k^{-1}lk \in J$ and so J is normal in G.

Consider the first part of a chief series of G passing through N, $1 = L_0 \leq L_1 \leq \ldots \leq L_s = N$. The length of the series up to N is $l_G(N)$. By the above all these subgroups L_i are isomorphic to normal subgroups of K. Then we have a normal series in K which may be refined to a chief series in K. Then $l_G(N) \leq l_K(N)$. As N is a normal subgroup of K then $l_K(N) \leq l(K)$ and so $l_G(N) \leq l(K)$ as required.

If $G \neq H \times K$ then without loss of generality $N \neq K$, and so $l_G(N) \leq l_K(N) < l(K)$. Then $l(G) < l(K) + l(H)$ in this case. □

Lemma 9.1.18. *A group G is a subdirect product of H_1, H_2 and H_3 if and only if there exists a subdirect product L of H_1 and H_2 such that G is a subdirect product of L and H_3.*

Proof. First consider the case where G is a subdirect product of H_1, H_2 and H_3. Let π_i be the projection map from G to H_i for $i = 1, 2, 3$. Let ϕ be the projection map from G to the first 2 coordinates, and let L be the image of this map. Then $G \leq L \times H_3$ where $G\phi = L$ and $G\pi_3 = H_3$. Clearly $L \leq H_1 \times H_2$. It remains to show that L is a subdirect product of H_1 and H_2. For every $h_1 \in H_1$, there exists (h_1, h_2, h_3) in G for some $h_2 \in H_2$ and $h_3 \in H_3$. Then by considering the projection onto the first two coordinates, it follows that for every h_1 in H_1, there exists h_2 in H_2 such that (h_1, h_2) is in L. That is, if ϕ_1 is the projection map from L to H_1 then $L\phi_1 = H_1$. A similar argument works for H_2, and so L is a subdirect product of H_1 and H_2.

Conversely, suppose G is a subdirect product of L and H_3, where L is a subdirect product of H_1 and H_2. Then $G \leq H_1 \times H_2 \times H_3$. Let π_i be the projection map from G to H_i for $i = 1, 2, 3$. Clearly $G\pi_3 = H_3$. For any $h_1 \in H_1$, there exists an $h_2 \in H_2$ such that $(h_1, h_2) \in L$ as L is a subdirect product of H_1 and H_2. Then as G is a subdirect product of L and H_3, there exists $h_3 \in H_3$ such that $(h_1, h_2, h_3) \in G$. So $G\pi_1 = H_1$. Similarly we may show that $G\pi_2 = H_2$, and so G is a subdirect product of H_1, H_2 and H_3. □

Lemma 9.1.19. *Let G be a subdirect product of $H_1, H_2, \ldots, H_k$. Then $l(G) \leq l(H_1) + l(H_2) + \ldots + l(H_k)$ with equality if and only if $G = H_1 \times \ldots \times H_k$.*

Proof. This holds when $k = 2$ by Lemma 9.1.17. Then we assume that $k > 2$, and the result holds for $k-1$. By Lemma 9.1.18, G is the subdirect product of $G_1 \times H_k$, for some subdirect product G_1 of $H_1, H_2, \ldots, H_{k-1}$. Then $l(G) \leq l(G_1) + l(H_k)$. By induction $l(G_1) \leq l(H_1) \times l(H_2) \times \ldots \times l(H_{k-1})$ and so $l(G) \leq l(H_1) + l(H_2) + \ldots + l(H_k)$. If G is not the full direct product $H_1 \times \ldots \times H_k$ then either $G_1 \neq H_1 \times \ldots \times H_k$ or $G \neq G_1 \times H_k$. Then it follows that $l(G) < l(H_1) \times \ldots \times l(H_k)$ in this case. □

Note that this result does not hold for arbitrary subgroups of direct products.

9.2 Random generation of finite groups

In this section we give some basic definitions in order to discuss results on random generation. In particular, we bound the number of random elements required to generate a group G with a given failure probability ϵ, in terms of $d(G)$ and the chief length $l(G)$. We give existing bounds on the minimal number of generators $d(G)$ for permutation and matrix groups. In the following chapters we will find bounds on the chief length $l(G)$ of permutation and matrix groups.

Definition 9.2.1. Let G be a group and define the following.

- $m_n(G)$ is the number of maximal subgroups of G of index n.
- $\mathcal{M}(G) = \max_{n \geq 2} \log m_n(G) / \log n$.

Recall $d(G)$ is the minimal number of generators for a group G, and $P_G(k)$ is the probability of generating G with k randomly chosen elements. We are interested in bounding the number of random elements required to generate G with a given probability.

Definition 9.2.2. Let $\epsilon \in (0, 1)$. Then define

$$d^{\epsilon}(G) = \min\{k \in \mathbb{N} : P_G(k) \geq 1 - \epsilon\}.$$

So $d^{\epsilon}(G)$ is the number of uniform random elements required to generate G with failure probability at most ϵ. This was initially studied for $\epsilon = (e-1)/e$ due to applications to the Product Replacement Algorithm [78]. We are interested in estimating $d^{\epsilon}(G)$ for any given $0 < \epsilon < 1$.

For example, the results in the first part of the thesis show that if G is a simple group and $\epsilon \geq 37/90$, then $d^{\epsilon}(G) = 2$. There is a bound for $d^{\epsilon}(G)$ which uses the Riemann zeta function.

Definition 9.2.3. The Riemann zeta function is defined to be $\zeta(t) = \sum_{n=1}^{\infty} 1/n^t$ for $t \in \mathbb{C}$ with $\Re(t) > 1$.

We are only interested in the case where t is real. Note that this is decreasing with increasing t and has limit 1, so for any $\epsilon \in (0,1)$ we may choose t such that $\zeta(t) \leq 1+\epsilon$. A slight modification of a theorem of Lubotzky [64] gives the following.

Theorem 9.2.4 ([64])**.** *Let $\epsilon \in (0,1)$ and let t be such that $\zeta(t) \leq 1+\epsilon$. Then*

$$d^{\epsilon}(G) \leq d(G) + 2\log l(G) + t + 2.$$

We shall give a brief outline of some of the theorems required to prove this. Note that for any ϵ we can always find an appropriate t as $\zeta(t)$ decreases with increasing t. Lubotzky's original theorem only considers the case where $\epsilon = (e-1)/e$ and uses the estimate $l(G) \leq \log|G|$. The proof combines the following.

Proposition 9.2.5 ([64, Proposition 1.2])**.** *Let $\epsilon = (e-1)/e$. Then $d^{\epsilon}(G) \leq \mathcal{M}(G) + 2.02$.*

Theorem 9.2.6 ([64, Theorem 2.1])**.** $\mathcal{M}(G) \leq d(G) + 2\log\log|G| + 2$.

The proof of Proposition 9.2.5 can be easily modified as follows.

Proposition 9.2.7. *Let $\epsilon \in (0,1)$ and let t be such that $\zeta(t) \leq 1+\epsilon$. Then*

$$d^{\epsilon}(G) \leq \mathcal{M}(G) + t.$$

Proof. By definition,

$$d^{\epsilon}(G) = \min\{k : P_G(k) \geq 1-\epsilon\} = \min\{k : 1 - P_G(k) \leq \epsilon\}.$$

We may bound $P_G(k)$ using maximal subgroups and so,

$$\begin{aligned} 1 - P_G(k) &\leq \sum_{M <_{\max} G} \frac{1}{[G:M]^k} \\ &= \sum_{n \geq 2} m_n(G) n^{-k} \\ &\leq \sum_{n \geq 2} n^{\mathcal{M}(G)} n^{-k} \\ &= \sum_{n \geq 2} n^{\mathcal{M}(G)-k}. \end{aligned}$$

If $k \geq \mathcal{M}(G) + t$, then

$$\sum_{n \geq 2} n^{\mathcal{M}(G)-k} \leq \sum_{n \geq 2} n^{-t} = \zeta(t) - 1.$$

As t has been chosen so that $\zeta(t) \leq 1+\epsilon$ then $1 - P_G(k) \leq \epsilon$ if $k \geq \mathcal{M}(G)+t$. As $d^{\epsilon}(G)$ is the minimum k such that $1 - P_G(k) \leq \epsilon$ then we must have $d^{\epsilon}(G) \leq \mathcal{M}(G) + t$. □

Looking at the proof of Theorem 9.2.6 we can see where the chief length of G appears and so we obtain

$$\mathcal{M}(G) \leq d(G) + 2\log l(G) + 2.$$

In fact, [64, Corollary 2.7] gives a slightly better bound on $\mathcal{M}(G)$ which is obtained by being more careful with some of the estimates in the proof. We have noted where the chief length appears in the proof and replaced it in the following.

Corollary 9.2.8 ([64, Corollary 2.7])**.** *Let $\rho(G)$ be the smallest index of a proper subgroup of G. Then*

$$\mathcal{M}(G) \leq \frac{1+\log l(G)}{\log \rho(G)} + \max\left(d(G), \frac{\log l(G)}{\log \rho(G)}\right) + 2.$$

Using the fact that the smallest index of a proper subgroup of G is at least 2, and combining with Proposition 9.2.7, we can improve the bound on $d^{\epsilon}(G)$ given in Theorem 9.2.4.

Theorem 9.2.9. *Let $\epsilon \in (0,1)$ and let t be such that $\zeta(t) \leq 1+\epsilon$. Then*

$$d^{\epsilon}(G) \leq \log l(G) + \max\{d(G), \log l(G)\} + t + 3.$$

We may subsititute existing bounds on $d(G)$ into Theorems 9.2.4 and 9.2.9 to bound $d^{\epsilon}(G)$. When G is a permutation group we have the following bound due to Neumann (but published in [13]).

Theorem 9.2.10 ([13])**.** *Let $G \leq S_n$. Then $d(G) \leq \max(2, \lfloor n/2 \rfloor)$.*

This can be improved when G is a subnormal subgroup of a primitive permutation group and also when G is almost simple.

Theorem 9.2.11 ([35, Theorem 1.1])**.** *Let G be a subnormal subgroup of a primitive permutation group of degree n. Then $d(G) \leq \log n$ unless $n = 3$ and $G \cong S_3$.*

Theorem 9.2.12 ([20])**.** *Let G be an almost simple group. Then $d(G) \leq 3$.*

Next we consider the case where G is a matrix group.

Theorem 9.2.13 ([47])**.** *Let G be a finite completely reducible matrix group of dimension n. Then $d(G) \leq \lfloor 3n/2 \rfloor$.*

This can be improved in specific cases.

Theorem 9.2.14 ([35, Theorem 1.2])**.**

1. *Let $G \leq \mathrm{GL}_n(F)$ be finite and completely reducible. If F does not contain a primitive fourth root of unity then $d(G) \leq n$. Furthermore, if $|F| = 2$ and $n > 3$ then $d(G) \leq n/2 + 1$.*

2. *Let H be a subnormal subgroup of a finite weakly quasiprimitive subgroup of $\mathrm{GL}_n(F)$, and let Z be the scalar subgroup of $\mathrm{GL}_n(F)$. Then $d(HZ/Z) \leq 2\log n$. Furthermore, if $|F| = 2$, then $d(H) \leq 2$ when $n \leq 5$ or $n = 7$, and $d(H) \leq 3$ when $n \leq 17$.*

Then we use these bounds on $d(G)$ to improve the bounds on $d^{\epsilon}(G)$. To further improve these bounds on random generation we seek better bounds on the chief length $l(G)$. If $G \leq S_n$, we seek bounds on $l(G)$ in terms of the degree n, if $G \leq \mathrm{GL}_n(q)$ we seek bounds in terms of the dimension n and the field size q. These cases are considered in the next two chapters.

Chapter 10

Random generation and chief length of permutation groups

In this chapter we consider the case where $G \leq S_n$, and bound the chief length $l(G)$ in terms of the degree n. As previously discussed we are interested in bounding $d^\epsilon(G)$, the number of random elements required to generate G with failure probability at most ϵ. As described in Chapter 9, $d^\epsilon(G)$ may be bounded in terms of $d(G)$, the minimum number of generators of G, and $l(G)$. We will use existing bounds on $d(G)$ (Theorems 9.2.10, 9.2.11, and 9.2.12). As mentioned earlier we may bound $l(G)$ by $\log |G|$, and hence by $n \log n$. We state existing bounds on the subgroup length and the composition length, which are upper bounds for the chief length, before determining tighter bounds on $l(G)$.

Theorem 10.0.1 ([13, Theorem 1]). *Let $f(G)$ be the maximal length of a chain of subgroups in a finite group G. Then $f(S_n) = \lfloor (3n-1)/2 \rfloor - b_n$ where b_n denotes the number of ones in the base 2 expansion of n.*

Lemma 10.0.2 ([27, Lemma 2]). *If G is a permutation group on n letters with s orbits, then the composition length of G is at most $(4/3)(n-s)$, and this bound can be attained by suitable permutation groups.*

As described in [27], this bound is achieved when $G = S_4 \operatorname{wr} S_4 \operatorname{wr} \ldots \operatorname{wr} S_4$, the iterated wreath product of i copies of S_4 acting imprimitively on $n = 4^i$ points. In this case G is transitive and $l(G) = 4^i + 4^{i-1} + \ldots + 4 = (4/3)(n-1)$.

Theorem 10.0.3 ([79, Theorem 2.10]). *Let G be a primitive subgroup of S_n. Then*

1. *The product of the orders of the abelian composition factors of G is at most $24^{-1/3} n^{1+c_0}$ (where $c_0 = 2.243\ldots$).*

2. *The number of non-abelian composition factors of G is at most $\log n$.*

Then as each composition factor has order at least two, the number of abelian factors is at most $\log(24^{-1/3}n^{1+c_0}) \leq 3.25 \log n$. Then the number of composition factors, and hence the number of chief factors may be bounded above.

Corollary 10.0.4. *The number of composition factors of a primitive subgroup G of S_n is bounded above by $4.25 \log n$.*

We seek to improve these bounds and in this section we prove the following two theorems. This leads to improved bounds on random generation as stated at the end of this chapter (Theorem 10.3.1).

Theorem 10.0.5. *Let G be a permutation group of degree n with s orbits. Then $l(G) \leq n - s$.*

Theorem 10.0.6. *If G is a primitive permutation group then one of the following holds.*

1. *G is of affine type and $l(G) \leq 2 \log n$.*
2. *G is a twisted wreath product and $l(G) \leq \log_{60} n$.*
3. *G is an almost simple group and $l(G) \leq \log \log n + \log 3 + 1$.*
4. *G is of diagonal type and $l(G) \leq \log_{60} n + 3$.*
5. *G is of product type and $l(G) \leq \log n$.*

We construct examples that achieve the bound given in Theorem 10.0.5 in Example 10.2.2. Theorem 10.2.5 shows that these groups, together with a couple of groups of small degree, are the only groups $G \leq S_n$, such that $l(G) = n - 1$.

We prove Theorems 10.0.5 and 10.0.6 together by induction on n. We use the O'Nan–Scott Theorem (2.1.25) to split our proof into separate cases.

10.1 Chief length of primitive permutation groups

We shall also use information on minimal normal subgroups and socles of primitive permutation groups, so we discuss this first before bounding the chief length of primitive groups. As we will eventually prove Theorems 10.0.5 and 10.0.6 together using induction, we will assume in many instances in this section that Theorem 10.0.5 holds in degree less than n.

Theorem 10.1.1 ([24, Theorem 4.3B])**.** *If G is a finite primitive subgroup of S_n, and K is a minimal normal subgroup of G, then exactly one of the following holds:*

1. *for some prime p and some integer d, K is a regular elementary abelian group of order p^d, and $\mathrm{Soc}(G) = K = C_G(K)$;*

2. *K is a regular non-abelian group, $C_G(K)$ is a minimal normal subgroup of G which is permutation isomorphic to K, and $\mathrm{Soc}(G) = K \times C_G(K)$;*

3. *K is non-abelian, $C_G(K) = 1$ and $\mathrm{Soc}(G) = K$.*

So a primitive permutation group has either one or two minimal normal subgroups. If G is almost simple then it has exactly one minimal normal subgroup $\mathrm{Soc}(G)$. An example of when G has two minimal normal subgroups is when $G = T \times T$ for some simple group T. If we consider this in its action on the cosets of the diagonal subgroup $D = \{(t, t) : t \in T\}$, then G is a primitive group of diagonal type. We prove the following which determines precisely when a primitive permutation group has 2 minimal normal subgroups

Lemma 10.1.2. *Let G be a primitive permutation group of degree n, with socle $\mathrm{Soc}(G) = T^k$ for some simple group T. Then G has exactly two minimal normal subgroups in precisely the following cases.*

1. *G is of diagonal type, $n = |T|$ and $T^2 \leq G \leq T^2.\mathrm{Out}(T)$.*

2. *G is of product type, $G \leq U \operatorname{wr} S_s$, where U is of diagonal type, $T^2 \leq U \leq T^2.\mathrm{Out}(T)$ and $n = |T|^s$.*

In all other cases G has a unique minimal normal subgroup.

Proof. By Theorem 10.1.1, G has at most 2 minimal normal subgroups. If G has two minimal normal subgroups K_1 and K_2 then $\mathrm{Soc}(G) = K_1 \times K_2$, $K_1 \cong K_2$ and as they are both regular $|K_i| = n$. In this case $\mathrm{Soc}(G)$ is not regular. We consider each of the cases from the O'Nan–Scott Theorem (2.1.25). If G is of affine type or a twisted wreath product then $\mathrm{Soc}(G)$ is regular and so in this case G can only have one minimal normal subgroup. If G is almost simple then $\mathrm{Soc}(G)$ is simple and is clearly the unique minimal normal subgroup of G. So it remains to consider the case where G is of diagonal type or of product type.

Consider the case where G is of diagonal type. Then $n = |T|^{k-1}$ and $G = T^k.H$ for H a subdirect product of $H_1 \leq S_k$ and $H_2 \leq \mathrm{Out}(T)$. The socle of G is $\mathrm{Soc}(G) = T^k$. For G to have two minimal normal subgroups, $|\mathrm{Soc}(G)| = n^2$ as each normal subgroup is regular, and this only occurs when $k = 2$. So suppose $k = 2$ and let $T^2 = T_1 \times T_2$. If $G \leq T^2.\mathrm{Out}(T)$, that is $H_1 = 1$, then T_1 and T_2 are both normal in G, and so these are the minimal normal subgroups of G. Otherwise suppose $H_1 = S_2$. Then conjugation of T_1 by the non-trivial element of S_2 sends T_1 to T_2 (and vice-versa), and so T_1 cannot be normal. Therefore in this case G has a unique minimal normal subgroup.

For the remainder of the proof we consider the case where G is a group of product type and so $G \leq U \operatorname{wr} S_s$, for U almost simple or of diagonal type.

Then $G = H.L$ for $H \leq U^s = U_1 \times \ldots \times U_s$, and L a transitive subgroup of S_s. The elements of G can be written in the form $(u_1, u_2, \ldots, u_s, \sigma)$ for $u_i \in U_i$ and $\sigma \in L$. First suppose U is almost simple. Then $\mathrm{Soc}(U) = T$, and $\mathrm{Soc}(G) = T^s = T_1 \times \ldots \times T_s$. Suppose K_1 and K_2 are distinct minimal normal subgroups of G. Then $K_1 = T^{s/2}$ which without loss of generality can be considered as $T_1 \times T_2 \times \ldots \times T_{s/2} \times 1 \times \ldots 1$. Conjugating this subgroup by $(u_1, u_2, \ldots, u_k, \sigma) \in G$ takes T_i to $T_{i\sigma}$. As L is transitive, we may take each T_i to T_j for any i, j. Then K_1 cannot be normal. So $\mathrm{Soc}(G) = T^s$ is the unique normal subgroup in this case.

Now consider the case where U is of diagonal type. Then $\mathrm{Soc}(U) = T^r$, $\mathrm{Soc}(G) = T^{rs}$, and G has degree $n = |T|^{(r-1)s}$. As described above, if G has 2 minimal normal subgroups then $|\mathrm{Soc}(G)| = n^2 = |T|^{2(r-1)s}$. This only happens when $r = 2$ and so we assume $r = 2$ for the rest of the proof. There are 2 cases to consider for U, where $T^2 \leq U \leq T^2.\mathrm{Out}(T)$, and where $U = T^2.A.S_2$ for $A \leq \mathrm{Out}(T)$.

Suppose $T^2 \leq U \leq T^2.\mathrm{Out}(T)$. Then $\mathrm{Soc}(U_i) = T_{2i-1} \times T_{2i}$ for $1 \leq i \leq s$, $\mathrm{Soc}(G) = T_1 \times \ldots \times T_s$, and by the diagonal type case above U_i has 2 minimal normal subgroups T_{2i-1} and T_{2i}. Consider the subgroup $N = T_1 \times T_3 \times \ldots \times T_{2s-1} \cong T^s \leq \mathrm{Soc}(G)$, the direct product of one minimal normal subgroup of each U_i. If G has 2 minimal normal subgroups they must each be isomorphic to T^s. If we can show that N is normal then we are done. Take an arbitrary element $g \in G$. Then $g = (u_1, \ldots, u_s, \sigma)$ for $u_i \in U_i$ $(1 \leq i \leq s)$, and $\sigma \in L$. Conjugation of N by g takes T_{2i-1} to T_{2j-1} where $i\sigma = j$. Together with the normality of T_{2i-1} in U_i, this implies that $N^g = N$, and so in this case G has two minimal normal subgroups.

Finally suppose $U = T^2.A.S_2$ for $A \leq \mathrm{Out}(T)$. Again $\mathrm{Soc}(U_i) = T_{2i-1} \times T_{2i}$. Consider the element $t = (t_1, 1, 1, \ldots, 1, 1) \in T^{2s} \leq G$ for $t_1 \in T$. Conjugating by an element $u = (u_1, \ldots u_s)$ of U^s, where u_1 projects onto the non-trivial element of S_2, gives $u^{-1}tu \in T_2$ which implies any normal subgroup containing T_1 contains T_2. Similarly, any subgroup containing T_{2i-1} contains T_{2i}. The transitivity of L means that we may choose $y = (y_1, y_2, \ldots, y_s, \sigma) \in G$ such that $1\sigma = 2i - 1$. Thus conjugating T_1 by such a y gives T_{2i-1}, that is, any normal subgroup containing T_1 contains T_{2i-1}. It follows that T^{2s} is the minimal normal subgroup of G. So if $G \leq U \mathrm{\ wr\ } S_s$ where U is of diagonal type of degree $|T|^{r-1}$, then G has 2 distinct normal subgroups if and only if $T^2 \leq U \leq T^2.\mathrm{Out}(T)$. □

So if G is a primitive permutation group then $l_G(\mathrm{Soc}(G)) = 1$ if G has a unique minimal normal subgroup, and $l_G(\mathrm{Soc}(G)) = 2$ otherwise. Now we will assume that Theorem 10.0.5 holds for degrees less than n, and bound the chief length of primitive permutation groups.

Lemma 10.1.3. *Let G be a primitive group of affine type of degree n. Then $l(G) \leq \min\{1 + (\log n)^2, n - 1\}$.*

Proof. If G is a group of affine type, then $G = \mathbb{F}_p^k \rtimes H$ where H is an irreducible subgroup of $\mathrm{GL}_k(p)$, and the degree of G is $n = p^k$. By Lemma 9.1.15, $l(G) = l_G(\mathbb{F}_p^k) + l(H)$. The minimal normal subgroup of G is $\mathbb{F}_p^k$ and so $l_G(\mathbb{F}_p^k) = 1$. The order of H is bounded above by $|\mathrm{GL}_k(p)| < p^{k^2}$. Using the fact that $k = \log_p n \leq \log n$, the chief length of H is bounded by $l(H) \leq \log |H| < \log p^{k^2} = k \log n$. So

$$l(G) \leq 1 + (\log n)^2.$$

This is bounded above by $n - 1$ when $n \geq 22$. We use MAGMA [8] to explicitly check chief lengths of primitive groups of affine type of degree less than 22 and in these cases we confirm that $l(G) \leq n - 1$. □

This proof shows that $l(G) \leq n - 1$ for a group $G \leq S_n$ of affine type. Later, in Lemma 10.2.1, we will use the result for the chief length of $H \leq \mathrm{GL}_k(q)$ (which uses Theorem 10.0.5), and we will improve the bound for groups of affine type.

Lemma 10.1.4. *Let G be an almost simple permutation group of degree n, where $G = S.A$ for $S = \mathrm{Soc}(G)$ and $A \leq \mathrm{Out}(S)$. If $n \leq 9$, and A is non-trivial, then $l(A) = 1$. If $n \leq 20$ then $l(A) \leq 2$, and if $n \leq 64$ then $l(A) \leq 3$.*

Proof. Lists of simple groups embedded in S_n for small n can be found in [24, Appendix B]. In some cases it will not be possible to embed all of $\mathrm{Out}(S)$ in S_n, so we just consider the possibilities for A. For example, if $S = A_6$ and $G \leq S_6$, then $A \leq C_2$. For $n \leq 9$, A must be either trivial or simple. If $n \leq 20$, then $|A| \leq 4$ and so $l(A) \leq 2$. If $n \leq 64$ then $|A| \leq 12$. Then A can have at most 3 chief factors, that is, $l(A) \leq 3$. □

Lemma 10.1.5. *Let G be an almost simple primitive group of degree n. Then $l(G) \leq \log \log n + \log 3 + 1 \leq n - 1$.*

Proof. If G is an almost simple group then $G = S.A$ for some non-abelian simple group S, and $A \leq \mathrm{Out}(S)$. Then $l(G) \leq l(S) + l(A)$. As S is simple, $l(S) = 1$. We bound $l(A)$ by $\log |A| \leq \log |\mathrm{Out}(S)|$. By Lemma 2.3.3, $|\mathrm{Out}(S)| \leq 3 \log n$ giving

$$\begin{aligned} l(A) &\leq \log |\mathrm{Out}(S)| \\ &\leq \log(3 \log n) \\ &\leq \log 3 + \log \log n. \end{aligned}$$

Then,

$$l(G) \leq \log \log n + \log 3 + 1.$$

As $n \geq 5$, this is bounded above by $n - 1$. □

Lemma 10.1.6. *Let G be a primitive group of degree n where G is a twisted wreath product, and assume Theorem 10.0.5 holds for permutation groups of degree less than n. Then $l(G) \leq \log_{60} n < n - 1$.*

Proof. If G is a twisted wreath product, then $n = |T|^k$ for some simple group T and some $k \geq 6$. The socle of G is T^k and $G = T^k.H$ where H is a transitive subgroup of S_k. By Lemma 9.1.15 the chief length of G is $l(G) = l_G(T^k) + l(H)$. By our assumption, as $k < n$, the chief length of H is bounded by $l(H) \leq k - 1$. By Lemma 10.1.2 the length of the socle is $l_G(T^k) = 1$. We bound $k = \log_{|T|} n \leq \log_{60} n$, and it follows that

$$l(G) \leq 1 + (k - 1) \leq \log_{60} n < n - 1.$$

□

Lemma 10.1.7. *Let G be a primitive group of degree n where G is of diagonal type, and assume that Theorem 10.0.5 holds for permutation groups of degree less than n. Then $l(G) \leq \log_{60} n + 3 < n - 1$.*

Proof. As G is of diagonal type, $G = T^k.H$ for some simple group T and a subgroup H which is a subdirect product of $H_1 \leq S_k$ and $H_2 \leq \mathrm{Out}(T)$. The degree of G is $n = |T|^{k-1}$ and so $k - 1 = \log_{|T|} n \leq \log_{60} n$ and $|T| \leq n$. By Lemmas 9.1.15 and 9.1.19,

$$l(G) = l_G(\mathrm{Soc}(G)) + l(H) \leq l_G(\mathrm{Soc}(G)) + l(H_1) + l(H_2).$$

If $G \leq T^2.\mathrm{Out}(T)$ then $l_G(\mathrm{Soc}(G)) = 2$, otherwise $l_G(\mathrm{Soc}(G)) = 1$ by Lemma 10.1.2. By assumption $l(H_1) \leq k - 1$.

Using Lemma 2.3.2,

$$\begin{aligned} l(H_2) &\leq \log |H_2| \\ &\leq \log |\mathrm{Out}(T)| \\ &\leq \log((6/7) \log |T|) \\ &\leq \log(6/7) + \log \log |T|. \end{aligned}$$

To improve the bound on $l(G)$ in small cases we use the fact that if T is a simple group and $|T| < 360$ then $|\mathrm{Out}(T)| = 2$, and if $|T| < 20160$ then $|\mathrm{Out}(T)| \leq 4$.

Consider the case where $k = 2$ and so $n = |T|$. Then either $l_G(\mathrm{Soc}(G)) = 2$ and $l(H_1) = 0$, or $l_G(\mathrm{Soc}(G)) = 1$ and $l(H_1) \leq 1$. Then

$$l(G) \leq 2 + l(H_2)$$

and so $l(G) \leq 2 + \log(6/7) + \log \log n$. If $|T| \geq 20160$, then $n \geq 20160$ and so

$$l(G) \leq 2 + \log(6/7) + \log \log n \leq \log_{60} n + 3.$$

If $|T| < 20160$ then $l(G) \leq 4 \leq \log_{60} n + 3$. So in all cases

$$l(G) \leq \log_{60} n + 3.$$

Now suppose $k \geq 3$, and so $n = |T|^{k-1}$, $k - 1 = \log_{|T|} n$, and $|T| \leq n^{1/2}$. Then

$$\begin{aligned} l(G) &\leq l_G(\mathrm{Soc}(G)) + l(H_1) + l(H_2) \\ &\leq 1 + (k-1) + l(H_2) \\ &\leq 1 + \log_{|T|} n + \log(6/7) + \log\log|T| \\ &\leq 1 + \log(6/7) + \log_{|T|} n + \log\log n^{1/2} \\ &\leq 1 + \log(6/7) + \log(1/2) + \log_{|T|} n + \log\log n \\ &\leq \log_{|T|} n + \log\log n + \log(6/7). \end{aligned}$$

If $|T| < 20160$, then $l(H_2) \leq 2$ and

$$l(G) \leq 1 + (k-1) + 2 \leq \log_{60} n + 3.$$

If $|T| \geq 20160$ then $n \geq 20160^2$ and

$$l(G) \leq \log_{20160} n + \log\log n + \log(6/7) \leq \log_{60} n + 3.$$

In all cases, $n \geq 60$, and so $\log_{60} n + 3 < n - 1$. □

Lemma 10.1.8. *Let G be a primitive group of degree n where G is of product type, and assume that Theorem 10.0.5 holds for permutation groups of degree less than n. Then $l(G) \leq \log n < n - 1$.*

Proof. Let $G \leq U \mathrm{wr} S_s$, where U is an almost simple group or a group of diagonal type of degree d. Then $G = H.L$ for H a subgroup of U^s, L a transitive subgroup of S_s, and $n = d^s$.

First suppose U is an almost simple group with socle T. By assumption, as $s < n$, the chief length of L is bounded by $l(L) \leq s - 1$. The socle of G is T^s and so $H = T^s.B$ where B is a subdirect product of A^s, for $A \leq \mathrm{Out}(T)$. Using Lemmas 9.1.15, 9.1.19 and 10.1.2,

$$\begin{aligned} l(G) &= l_G(T^s) + l(G/T^s) \\ &= l_G(T^s) + l(B.L) \\ &\leq l_G(T^s) + s \cdot l(A) + l(L) \\ &\leq 1 + s \cdot l(A) + (s-1) \\ &= s(l(A)+1). \end{aligned} \tag{10.1.1}$$

We may bound $l(A)$ by $\log|A| \leq \log|\mathrm{Out}(T)|$. As $T \leq U \leq S_d$, by Lemma 2.3.3, $|\mathrm{Out}(T)| \leq 3\log d$ and so $l(A) \leq \log(3\log d)$. Then

$$l(G) \leq s(\log(3\log d) + 1) = s\log(6\log d).$$

For smaller values of d we use the Lemma 10.1.4 and Equation (10.1.1) to estimate $l(A)$ and hence $l(G)$. Recall $n = d^s$. If $d \leq 9$, then

$$l(G) \leq 2s \leq \log 5^s \leq \log n.$$

If $10 \leq d \leq 20$, then

$$l(G) \leq 3s \leq \log 10^s \leq \log n.$$

If $21 \leq d \leq 63$, then

$$l(G) \leq 4s \leq \log 21^s \leq \log n.$$

Finally if $d \geq 64$, then

$$l(G) \leq s \log(6 \log d) \leq \log d^s \leq \log n.$$

So if G is a primitive group of product type, with U almost simple, then

$$l(G) \leq \log n.$$

Now suppose that U is a primitive subgroup of diagonal type. Then the degree of U is $d = |T|^{(r-1)}$ for some $r \geq 2$, and the degree of G is $n = |T|^{(r-1)s}$. By assumption $l(L) \leq s - 1$. The socle of G is T^{rs} and so $H = T^{rs}.K$ where K is subdirect product of $A^s \times R^s$ for $A \leq \mathrm{Out}(T)$ and $R \leq S_r$. Then $G = T^{rs}.K.L$. Using Lemma 2.3.2,

$$l(A) \leq \log |A| \leq \log |\mathrm{Out}(T)| \leq \log \log |T|.$$

By Lemma 9.1.15 and Lemma 10.1.2,

$$\begin{aligned} l(G) &\leq l_G(\mathrm{Soc}(G)) + l(K) + l(L) \\ &\leq 2 + s - 1 + l(K) \\ &\leq 1 + s + l(K). \end{aligned}$$

By Lemma 9.1.19 and the inductive assumption,

$$l(K) \leq s \cdot l(A) + s \cdot l(R) \leq s \log \log |T| + s(r-1).$$

Then,

$$\begin{aligned} l(G) &\leq 1 + s + l(K) \\ &\leq 1 + s \log \log |T| + s + s(r-1) \\ &= 1 + s \log \log |T| + sr \\ &\leq s(\log \log |T| + r + 1) \\ &= s(\log \log |T| + \log 2^{r+1}) \\ &= s(\log(2^{r+1} \log |T|)) \\ &\leq s(\log |T|^{r-1}) \\ &= \log |T|^{(r-1)s} \\ &= \log n. \end{aligned}$$

So, for any primitive permutation group of product type,

$$l(G) \leq \log n < n - 1.$$

□

10.2 Proof of Theorems 10.0.5 & 10.0.6

We combine the lemmas on primitive groups from the previous section to prove Theorems 10.0.5 & 10.0.6 and bound the chief length of permutation groups.

Proof of Theorem 10.0.5. We prove this theorem by induction on n. If $n = 1$ then $l(G) = 0$. If $n = 2$ either $G = 1$ and so $l(G) = 0$, or $G = S_2$ and $l(G) = 1$. So the result holds in these cases. Now assume that $n > 2$ and that the result holds for permutation groups of degree less than n.

First we consider the case where G is primitive. By the O'Nan–Scott Theorem (2.1.25), G is one of the following: affine type, a twisted wreath product, almost simple, diagonal type or product type. Together with this inductive assumption, Lemmas 10.1.3, 10.1.5, 10.1.6, 10.1.7 and 10.1.8, show that $l(G) \leq n - 1$ in all these cases.

Next consider the case where G is intransitive acting on s orbits of lengths $n_1, n_2, \ldots, n_s$. So $n = n_1 + n_2 + \ldots + n_s$. Then G is a subdirect product of $H_1, H_2, \ldots, H_s$, where H_i is a transitive permutation group of degree n_i. By Lemma 9.1.19, $l(G) \leq l(H_1)+l(H_2)+\ldots+l(H_s)$. By induction $l(H_i) \leq n_i-1$ and so $l(G) \leq n - s$.

Finally consider the case where G is transitive but imprimitive with t blocks of size b. So $n = bt$ for some $b, t \geq 2$. If H corresponds to the action of G on a block, and K is the group induced by G which permutes the blocks, then $G \leq H \operatorname{wr} K$. As H^t is normal in $H \operatorname{wr} K$, then $H^t \cap G$ is normal in G. As $G/(H^t \cap G) \cong K$, then by Lemma 9.1.15

$$l(G) = l_G(H^t \cap G) + l(K) \leq l(H^k \cap G) + l(K).$$

The group K is a permutation group of degree $t < n$, and so by induction $l(K) \leq t - 1$. As H is the group which corresponds to the action of G on a block of size b, $H \leq S_b$, and it follows that H^t is a permutation group of degree bt with t orbits. Then $H^t \cap G$ is a permutation group of degree bt with at least t orbits, and by the result in the intransitive case $l(H^t \cap G) \leq bt - t$. Then

$$l(G) \leq (bt - t) + (t - 1) = n - 1$$

as required. □

This result is used in the next chapter to prove that if $H \leq \mathrm{GL}_d(q)$ is a completely reducible subgroup, then $l(H) \leq d + d \log q - 1$ (Theorem 11.0.4).

The proof of this only requires Theorem 10.0.5 which bounds the chief length of arbitrary permutation groups, and it does not require the tighter bounds on primitive permutation groups given in Theorem 10.0.6. In particular this bound for completely reducible matrix groups does not require the following lemma on the chief length of primitive permutation groups of affine type. We use Theorem 11.0.4 to improve Lemma 10.1.3, and give a tighter bound on $l(G)$ where $G \leq S_n$ is a group of affine type.

Lemma 10.2.1. *Let G be a primitive group of affine type of degree n. Then $l(G) \leq 2 \log n$.*

Proof. If G is a group of affine type, then $G = \mathbb{F}_p^k \rtimes H$ where H is an irreducible subgroup of $\mathrm{GL}_k(p)$. By Lemma 9.1.15, $l(G) = l_G(\mathbb{F}_p^k) + l(H)$. As $\mathbb{F}_p^k$ is the minimal normal subgroup of G then $l(G) \leq 1 + l(H)$. Then by Theorem 11.0.4, $l(G) \leq l(H) + 1 \leq k + k \log p$ as H is an irreducible subgroup of $\mathrm{GL}_k(p)$. Then

$$l(G) \leq k + \log p^k \leq 2 \log n.$$

□

Then we prove Theorem 10.0.6, and give tighter bounds on $l(G)$ for primitive groups G.

Proof of Theorem 10.0.6. Combining Theorem 10.0.5 with Lemmas 10.1.5, 10.1.6, 10.1.7, 10.1.8, 10.2.1 allows us to bound $l(G)$ for primitive groups $G \leq S_n$. □

The bounds from Theorem 10.0.5 may be achieved for intransitive and imprimitive groups as described in the following example.

Example 10.2.2. Let $W_i = S_2 \operatorname{wr} S_2 \operatorname{wr} \ldots \operatorname{wr} S_2$, the iterated wreath product of i copies of S_2. Consider an imprimitive action on $n = 2^i$ points. The order of this group is $|W_i| = 2^{2^{i-1}+2^{i-2}+\ldots+1}$. As this is a 2-group,

$$l(W_i) = \log |W_i| = 2^{i-1} + 2^{i-2} + \ldots + 1 = 2^i - 1 = n - 1.$$

Consider a direct product of iterated wreath products of this form, $G = W_{i_1} \times W_{i_2} \times \ldots \times W_{i_s}$, where each W_{i_j} is acting on n_j points. Then G is an intransitive group acting on $n = n_1 + n_2 + \ldots + n_s$ points with s orbits. Then

$$l(G) = l(W_{i_1}) + \ldots + l(W_{i_s}) = n - s.$$

Note that a Sylow 2-subgroup of S_n is a direct product of iterated wreath products of this form, and so a Sylow 2-subgroup of S_n (for any n) achieves the upper bound $l(G) \leq n - s$ for the chief length.

In fact, we may show that Sylow 2-subgroups of S_{2^i}, and 2 groups of small degree (S_3 and S_4) are in fact the only permutation groups achieving the bound $l(G) = n - 1$ and so we may strengthen the bound on the chief length from Theorem 10.0.5. We will use the following two lemmas.

Lemma 10.2.3 ([15, Lemma 4])**.** *Let S_n be the symmetric group on n symbols. Then the Sylow 2-subgroups of S_n are self-normalising.*

Lemma 10.2.4. *Let $G = S_m \operatorname{wr} S_k$ be an imprimitive permutation group of degree $n = mk$. Let $2 \leq m, k \leq 4$. If $G \neq S_2 \operatorname{wr} S_2$ then $l(G) \leq n - 2$.*

Proof. We verify using Magma [8] that all these imprimitive groups G have chief length at most $n - 2$. □

Theorem 10.2.5. *Let G be a permutation group of degree n acting on s orbits. For $1 \leq j \leq s$, let G_j be the group induced by the action of G on the jth orbit, so that G is a subdirect product of $G_1 \times \ldots \times G_s$. Then*

$$l(G) \leq n - s.$$

Furthermore, this inequality is strict except when $G = G_1 \times \ldots \times G_s$ and for $1 \leq j \leq s$, G_j is one of the following.

1. *$G_j = S_3$ acting on 3 points.*
2. *$G_j = S_4$ acting on 4 points.*
3. *$G_j = W_i$ for some $i \geq 1$, where $W_i = \mathrm{Syl}_2(S_{2^i})$.*

Proof. Let $\mathcal{S} = \{S_3, S_4, W_i \text{ for } i \geq 1\}$ where these groups act on 3, 4 and 2^i points respectively. All these groups are transitive and it is easy to verify that $l(G) = n - 1$, for $G \in \mathcal{S}$. Now let G be a counter example of minimal degree.

First suppose that G is primitive, and so $G = G_1$. If G is primitive and not of affine type then by Theorem 10.0.6, $l(G) \leq n - 2$. If G is primitive of affine type then $l(G) \leq \lfloor 2 \log n \rfloor \leq n - 2$ for $n \geq 8$. Using Magma [8], we obtain all groups of affine type of degree at most 7 and see that if $G \notin \mathcal{S}$ then $l(G) \leq n - 2$.

Next suppose that G is transitive but imprimitive and so once again $G = G_1$. If G acts on k blocks of size m, by Theorem 2.1.15, $G \leq H \operatorname{wr} K$ for some transitive groups $H \leq S_m$ and $K \leq S_k$. By Lemma 2.1.16, $H^k \cap G$ is normal in G, and is a subdirect product of N^k for some $N \trianglelefteq H$. As $G/(H^k \cap G) \cong K$, by Lemmas 9.1.15 and 9.1.19,

$$\begin{aligned} l(G) &\leq l(H^k \cap G) + l(K) \\ &\leq k \cdot l(N) + l(K). \end{aligned}$$

As N has degree m, and K has degree k, if $l(G) = n-1$ this forces $l(N) = m-1$, $l(K) = k-1$, and $(H^k \cap G) = N^k$, the full direct product. The minimality of G forces $N, K \in \mathcal{S}$. By Lemma 10.2.3, W_i is self normalising in S_{2^i}. As $N \leq H \leq N_{S_m}(N)$, then $N = H$. So $G = H \operatorname{wr} K$, with $H, K \in \mathcal{S}$. Note that $W_{i+j} \cong W_i \operatorname{wr} W_j$, $W_i \operatorname{wr} S_k \cong W_{i-1} \operatorname{wr}(S_2 \operatorname{wr} S_k)$, and similarly $S_m \operatorname{wr} W_i \cong (S_m \operatorname{wr} S_2) \operatorname{wr} W_{i-1}$. The minimality of G implies $H, K \in \{S_2, S_3, S_4\}$. By assumption $G \neq S_2 \operatorname{wr} S_2 = W_2$.

By Lemma 10.2.4 we see that none of these possibilities satisfy $l(G) = n-1$ and so we obtain $l(G) \leq n-2$ if G is imprimitive and $G \neq W_i$. So if G is transitive and $G \notin \mathcal{S}$, then $l(G) \leq n-2$.

It is left to consider the case where G is intransitive. Then $s \geq 2$. If G_j has degree n_j, then $n = n_1 + \ldots + n_s$. By Lemma 9.1.19,

$$l(G) \leq l(G_1) + l(G_2) + \ldots + l(G_s)$$

with equality if and only if $G = G_1 \times \ldots \times G_s$. Then as $l(G_j) \leq n_j - 1$, if $l(G) = n - s$ then $l(G_j) = n_j - 1$ for $1 \leq j \leq s$ and $G = G_1 \times \ldots \times G_s$. As G_j is transitive for each j, by the above, $G_j \in \mathcal{S}$ for all j. Then the result holds. □

10.3 Random generation of permutation groups

Returning to random generation, we use our improved bounds on the chief length to improve bounds on $d^e(G)$ when $G \leq S_n$. We do this by combining the bounds on $d^e(G)$ from Theorems 9.2.4 and 9.2.9 with the bounds on $d(G)$ from Theorems 9.2.10, 9.2.11 and 9.2.12 and the bounds on $l(G)$ from Theorem 10.0.5. In all cases other than the almost simple case, the bound for $d(G)$ is greater than the bound for $\log l(G)$ and so we substitute our values of $l(G)$ into the bound for $d^e(G)$ from Theorem 9.2.9. In the almost simple case

$$\max\{d(G), \log l(G)\} \leq \max\{3, \log(\log\log n + \log 3 + 1)\}.$$

As $\log(\log\log n + \log 3 + 1) \geq 3$ but only for large n (n must be greater than 6.9×10^{12}), it is simpler to state the theorem using the bounds on $d^e(G)$ from Theorem 9.2.4.

Theorem 10.3.1. *Let $\epsilon \in (0,1)$ and let t be such that $\zeta(t) \leq 1 + \epsilon$. Let G be a permutation group of degree n with s orbits. Then*

$$d^e(G) \leq n/2 + \log(n-s) + t + 3.$$

If G is a primitive permutation group then one of the following holds.

1. *G is of affine type and*

$$d^e(G) \leq \log n + \log\log n + t + 4.$$

2. G is a twisted wreath product and

$$d^{\epsilon}(G) \leq \log n + \log \log_{60} n + t + 3.$$

3. G is an almost simple group and

$$d^{\epsilon}(G) \leq 2 \log(\log \log n + \log 3 + 1) + t + 5.$$

4. G is of diagonal type and

$$d^{\epsilon}(G) \leq \log n + \log(\log_{60} n + 3) + t + 3.$$

5. G is of product type and

$$d^{\epsilon}(G) \leq \log n + \log \log n + t + 3.$$

Chapter 11

Random generation and chief length of matrix groups

In this chapter we bound the chief length, $l(G)$, of completely reducible matrix groups $G \leq \mathrm{GL}_n(q)$ in terms of n and q, and use this to bound $d^{\epsilon}(G)$. There are existing bounds on the composition length (and hence the chief length) for specific types of matrix groups, for example in [65] and [48]. Recall $c(G)$ denotes the composition length of G.

Theorem 11.0.1 ([65, Theorem C])**.** *For each field K which has finite degree over its prime subfield, there is a number c_K such that if G is a finite completely reducible linear group of degree n over K then $c(G) \leq c_K n$. Moreover, there are two real numbers d_1 and d_2, independent of the field, such that $c_K = d_1 \log |K|$ if K is finite, and $c_K = d_2 \log[K : \mathbb{Q}]$ if K is a number field.*

Recall the definition of a quasiprimitive matrix group from Section 2.2.

Theorem 11.0.2 ([48, Theorem B])**.** *Let K be a field of order p^d, V a K-vector space of dimension n, G a quasiprimitive subgroup of $\mathrm{GL}_K(V)$. Then*

$$c(G) \leq \log p \max\left\{1, \frac{c_2 nd}{\log(nd)}\right\}$$

where c_2 is an absolute positive constant.

However, these bounds are not useful for us as they are given in terms of unspecified constants and we seek an explicit bound. For a matrix group $G \leq \mathrm{GL}_n(q)$, the chief length is bounded by,

$$l(G) \leq \log |G| \leq \log |\mathrm{GL}_n(q)| \leq n^2 \log q.$$

In fact, for an arbitrary matrix group we cannot do much better. Consider the following example.

Example 11.0.3. Let $G \leq \mathrm{GL}_n(q)$ be the group of matrices of the form

$$\begin{pmatrix} 1 & * & \dots & * \\ 0 & 1 & * & \vdots \\ \vdots & \ddots & \ddots & * \\ 0 & \dots & 0 & 1 \end{pmatrix},$$

that is, the matrices with ones down the diagonal, zeros below the diagonal, and entries above the diagonal can take any values in $\mathbb{F}_q$. Let $q = p^e$ for some prime p. This group has order $q^{n(n-1)/2}$. As it is a p-group (in fact, this is the Sylow p-subgroup of $\mathrm{GL}_n(q)$),

$$l(G) = \log_p |G| = (n(n-1)\log_p q)/2.$$

Asymptotically this bound is no better than the bound $l(G) \leq \log |G|$, and if $q = 2^e$, then $l(G) = \log |G|$. Thus we cannot hope to obtain a much better bound for the chief length of an arbitrary matrix group. So we consider completely reducible matrix groups and try to improve the bound on the chief length of these groups. In this case we can use the structure of primitive matrix groups (in fact, we use the weaker condition of these groups being weakly quasiprimitive), then use induction for the irreducible and completely reducible cases.

In this chapter we prove the following bound.

Theorem 11.0.4. *Let $G \leq \mathrm{GL}_n(q)$ be a completely reducible matrix group acting on $V = V_1 \oplus \cdots \oplus V_s$, where G acts irreducibly on each vector subspace V_i. Then*

$$l(G) \leq n + n \log q - s.$$

If in addition G is weakly quasiprimitive and $n \geq 2$, then

$$l(G) \leq (\log n)^2/2 + 4 \log n + n \log q.$$

Note that the second bound given is not smaller for small values of n. We prove this theorem by induction on the dimension n. First we prove the base case which will be used throughout. Note that if $G \leq \mathrm{GL}_1(q)$, then G acts on a one dimensional vector space $V = \mathbb{F}_q$. In this case G must act irreducibly on V.

Lemma 11.0.5. *Let $G \leq \mathrm{GL}_1(q)$. Then $l(G) \leq \log(q-1)$.*

Proof. Note that $\mathrm{GL}_1(q) \cong \mathbb{F}_q^\times$. Then

$$l(G) \leq \log |G| \leq \log |\mathrm{GL}_1(q)| \leq \log(q-1).$$

□

In particular, this shows that if $n = 1$, then $l(G) \leq n + n \log q - 1$. We use induction to prove the general bound for the chief length of completely reducible matrix groups and then we combine these bounds on the chief length, with bounds on the minimal number of generators $d(G)$ (Theorem 9.2.13 and Theorem 9.2.14), to improve the bound on the number of random generators $d^{\epsilon}(G)$. These bounds are given at the end of this chapter (Theorem 11.3.1).

11.1 Chief length of weakly quasiprimitive groups

Recall from Chapter 2 that the generalised Fitting subgroup $F^*(G)$ of a group G is defined to be $F^*(G) = F(G)E(G)$, where $F(G)$ is the largest nilpotent normal subgroup of G, and $E(G)$ is the subgroup generated by the subnormal quasisimple subgroups of G. It follows from Lemma 2.0.26 that $F^*(G)$ is the central product of groups $O_r(G)$ for primes r dividing $|G|$, and quasisimple subnormal subgroups S.

Lemma 11.1.1. *Let S be a subnormal quasisimple subgroup of a group G. Then the following hold.*

- *For all $g \in G$, S^g is a subnormal quasisimple subgroup of G.*
- *The normal closure $T = \langle S \rangle^G$ is a central product of $t \geq 1$ isomorphic quasisimple subnormal subgroups.*

Proof. As $S \cong S^g$, then the group S^g is also quasisimple. As S is a subnormal subgroup, there exists a subnormal series $S = N_0 < N_1 < \ldots < N_k = G$, where each N_i is a normal subgroup of N_{i+1}. Then $S^g = N_0^g < N_1^g < \ldots < N_k^g = G$ is a subnormal series from S^g to G, and thus S^g is also a subnormal subgroup.

Let S have t distinct conjugates, $S_1, S_2, \ldots, S_t$. By the above, these are all isomorphic quasisimple subnormal subgroups of G. By Lemma 2.0.26, the central product $S_1 \circ S_2 \circ \ldots \circ S_t$ is a subgroup of G. As T is the normal closure of S, then $T = \langle S_1, \ldots, S_t \rangle$ and it follows that T is the central product of $t \geq 1$ isomorphic copies of a quasisimple subnormal subgroup. □

As $Z(G)$ is abelian, it is nilpotent and contained in $F(G)$, and hence in $F^*(G)$. Then it follows from this, together with Lemma 2.0.26 and the previous lemma, that $F^*(G)$ is the central product of $Z(G)$, non-central normal subgroups $O_{r_i}(G)$ for some primes $r_1, \ldots, r_c$ dividing $|G|$, and normal subgroups $T_1, \ldots, T_k$, where each T_i is a central product of $t_i \geq 1$ subnormal quasiprimitive groups.

We discuss preliminary results before bounding the chief length of weakly quasisimple groups in Lemmas 11.1.17 and 11.1.18. First we show that we may bound the chief length of G in terms of the central factors of $F^*(G)$. We will require the following preliminary lemma.

Lemma 11.1.2. *Let $L \trianglelefteq G$. Then $C_G(L) \trianglelefteq G$.*

Proof. Let $c \in C_G(L)$, $g \in G$, and $l \in L$. Then the normality of L implies that $glg^{-1} = l'$ for some $l' \in L$. We need to show that $g^{-1}cg \in C_G(L)$, that is, $(g^{-1}cg)l(g^{-1}cg)^{-1} = l$. So,

$$\begin{aligned}(g^{-1}cg)l(g^{-1}cg)^{-1} &= g^{-1}cglg^{-1}c^{-1}g \\ &= g^{-1}cl'c^{-1}g \\ &= g^{-1}cc^{-1}l'g \\ &= g^{-1}l'g \\ &= l\end{aligned}$$

as required. □

Then we may construct the factor groups $G/C_G(L)$ for $L \trianglelefteq G$.

Lemma 11.1.3. *Let G be a group and suppose $F^*(G)$ is the central product of normal subgroups $L_1, \ldots, L_k$ and $Z(G)$, where $L_i \not\leq Z(G)$. Let $K = C_G(F^*(G))$. Then*

$$l(G/K) \leq \sum_{i=1}^{k} l(G/C_G(L_i)).$$

Proof. Note that $K = \bigcap_{i=1}^{k} C_G(L_i)$. Let $\bar{H}$ denote H/K for any subgroup H of G containing K. Consider projection maps

$$\pi_i : G/K \to G/C_G(L_i).$$

Let

$$\bar{K} = \bar{N}_0 \lhd \ldots \lhd \bar{N}_l = \bar{G}$$

be a chief series for $\bar{G}$. For $0 \leq j \leq l$, each $\bar{N}_j\pi_i$ is a normal subgroup of $G/C_G(L_i)$. If $j \neq 0$, then $\bar{N}_j\pi_i$ is a non-trivial subgroup of $G/C_G(L_i)$ for at least one i (otherwise $N_j \leq \bigcap_{i=1}^{k} C_G(L_i) = K$, a contradiction).

Then for each i we get the following chains of subgroups,

$$\bar{N}_0\pi_i \leq \bar{N}_1\pi_i \ldots \leq \bar{N}_l\pi_i = G/C_G(L_i).$$

Removing repetitions we obtain a normal series for $G/C_G(L_i)$ which can then be refined to a chief series for $G/C_G(L_i)$.

For $0 \leq j \leq l-1$, $\bar{N}_j\pi_i \neq \bar{N}_{j+1}\pi_i$ for at least one i (otherwise this would force $\bar{N}_j = \bar{N}_{j+1}$). So each subgroup $\bar{N}_j$ in the composition series for $\bar{G}$ corresponds to at least one subgroup $\bar{N}_j\pi_i$ in the chief series for some $G/C_G(L_i)$, where the series is constructed as described above. Then

$$l(G/K) \leq \sum_{i=1}^{k} l(G/C_G(L_i)).$$

□

We use the following theorems to describe irreducible modules for $F^*(G)$ in terms of irreducible modules for its central factors.

Theorem 11.1.4 ([30, Chapter 3, Theorem 7.1])**.** *Let $G = H \times K$ and let F be a splitting field for both H and K. If V and W are irreducible H and K modules, respectively, then the product module $V \otimes W$ is an irreducible FG-module. Conversely, every irreducible FG-module is equivalent to a product module of this form.*

Theorem 11.1.5 ([30, Chapter 3, Theorem 7.2])**.** *A central product $G = H \circ K$ of H and K can be identified with G^*/N^*, where $G^* = H \times K$ and N^* is a suitable normal subgroup of G^*. Then any FG-module is an FG^*-module in which N^* is in the kernel, and conversely.*

The following lemma comes from [44, Lemmas 2.10.1 & 5.5.5].

Lemma 11.1.6. *Let G be the central product of groups $L_1, \ldots, L_k$, and suppose G embeds absolutely irreducibly in $\mathrm{GL}_n(F)$. Let V be the natural module $V = F^n$. Then there is a tensor product decomposition $V = V_1 \otimes \cdots \otimes V_k$, such that L_i embeds absolutely irreducibly in $\mathrm{GL}(V_i)$.*

We shall use these lemmas to bound the chief length of $G \leq \mathrm{GL}_n(q)$ in terms of n (and q), by bounding the chief length of $G/C_G(O_{r_i}(G))$ and $G/C_G(T_i)$ in terms of the dimensions of the respective absolutely irreducible modules for $O_{r_i}(G)$ and T_i. The groups $G/C_G(O_{r_i}(G))$ and $G/C_G(T_i)$ can be described.

Lemma 11.1.7 ([35, Lemma 2.16])**.** *Let G be finite with cyclic centre Z, and assume that all abelian characteristic subgroups of G are contained in Z. Each non-central $O_r(G)$ is the central product of its intersection with Z and an extraspecial r-group E, of order r^{1+2m} say. If r is odd then E has exponent r. Any non-trivial absolutely irreducible module for E has dimension r^m, and $G/C_G(O_r(G)) \leq r^{2m}.\mathrm{Sp}_{2m}(r)$. Finally, the action of G/EZ on EZ/Z is completely reducible.*

Now suppose $G \leq \mathrm{GL}_n(q)$ where $Z(G) = Z(\mathrm{GL}_n(q)) \cap G$, and all abelian characteristic subgroups of G are contained in $Z(G)$. If M_r is an absolutely irreducible module for $O_r(G)$ then it follows from Lemma 11.1.6 and Lemma 11.1.7 that $\dim(M_r)$ is the product of dimensions of absolutely irreducible modules for E and $Z \cap O_r(G)$ (where E and Z are as in the previous lemma). Then as an irreducible module for $Z(G)$ has dimension 1, $\dim(M_r) = r^{2m}$ for some m.

Lemma 11.1.8 ([35, Lemma 2.17])**.** *Let $G \leq \mathrm{GL}_n(F)$, and let $L = F^*(G)$. Let T_i be a central factor of $F^*(G)$, where T_i is normal, and the central product of t_i isomorphic copies of some quasisimple group S_i. Let M_{T_i} be an irreducible module for T_i. Assume that F is a splitting field for all central*

factors of L, and that L acts homogeneously. Then M_{T_i} is a tensor product of t_i copies of some faithful irreducible FS_i-module M_{S_i}. Also, $G/C_G(T_i) \leq A \operatorname{wr} \mathrm{Sym}(t_i)$, where A is the subgroup of $\mathrm{Aut}(S_i/Z(S_i))$ that stabilises the module M_{S_i}.

It follows that $\dim M_{T_i} = s_i^{t_i}$, where s_i is the dimension of some irreducible module for S_i.

Lemma 11.1.9 ([35, Lemma 2.13])**.** *Let $G \leq \mathrm{GL}_n(F)$ be irreducible and weakly quasiprimitive and suppose that G has an abelian characteristic subgroup not contained in $Z(\mathrm{GL}_n(F))$. Then G has a characteristic subgroup K such that K is isomorphic to a subgroup K_1 of $\mathrm{GL}_{n/f}(F_1)$, for some divisor f of n and some extension F_1 of F where $[F_1 : F] = f$. All characteristic abelian subgroups of K_1 are contained in $Z(\mathrm{GL}_{n/f}(F_1))$, and K_1 is weakly quasiprimitive. Furthermore G/K is abelian of order at most f, and embeds naturally in $\mathrm{Gal}(F_1/F)$.*

Now we bound $l(G/C_G(O_{r_i}(G))$ and $l(G/C_G(T_i))$.

Lemma 11.1.10. *Let $H = r^{2m}.K$ for some prime r, where K is a completely reducible subgroup of $\mathrm{Sp}_{2m}(r)$, and assume Theorem 11.0.4 holds in dimensions up to $2m$. Then $l(H) \leq 2m + 2m \log r$.*

Proof. By Lemma 9.1.15, $l(H) = l_H(r^{2m}) + l(K)$. The subgroup K acts completely reducibly on the vector space $V = \mathbb{F}_r^{2m}$. Suppose $V = V_1 \oplus \cdots \oplus V_k$ as a sum of irreducible subspaces. Then $l_H(V) = k$ and $l(K) \leq 2m + 2m \log r - k$ by Theorem 11.0.4. So $l(H) \leq 2m + 2m \log r$ as required. □

Lemma 11.1.11. *Let $H = r^{2m}.K$ for some prime r, where K is a completely reducible subgroup of $\mathrm{Sp}_{2m}(r)$, and assume $r^m \leq 5$. Then $l(H)$ is bounded as follows.*

- *If $r = 2$ and $m = 1$, then $l(H) \leq 4$.*
- *If $r = 2$ and $m = 2$, then $l(H) \leq 8$.*
- *If $r = 3$ and $m = 1$, then $l(H) \leq 5$.*
- *If $r = 5$ and $m = 1$, then $l(H) \leq 5$.*

Proof. By Lemma 9.1.15, $l(H) \leq l(r^{2m}) + l(K) \leq 2m + l(K)$. The possibilities for r and m are limited and so using Magma we determine all subgroups K of $\mathrm{Sp}_{2m}(r)$ in each case. If $K \leq \mathrm{Sp}_2(2)$ then $l(K) \leq 2$, if $K \leq \mathrm{Sp}_4(2)$ then $l(K) \leq 4$, if $K \leq \mathrm{Sp}_2(3)$ then $l(K) \leq 3$, and finally if $K \leq \mathrm{Sp}_2(5)$ then $l(K) \leq 3$. The bounds on $l(H)$ follow. □

Lemma 11.1.12. *Let S be a quasisimple group that embeds absolutely irreducibly in $\mathrm{GL}_s(q)$, let A be an almost simple group with socle $S/Z(S)$, and let $B = (S/Z(S))^t$. Let $B \leq H \leq A \operatorname{wr} K$ for $K \leq S_t$. Then*

$$l(H) \leq \min\{(2 + \log(6/7))t + 2\log s^t + t\log\log q - 1,$$
$$(2 + \log 3)t + \log s^t + t\log\log q - 1\}.$$

Proof. The subgroup $H \cap A^t$ is normal in H and $H/(H \cap A^t) \cong K$ for some $K \leq S_t$. Then using Lemma 9.1.15 and Theorem 10.0.5

$$l(H) \leq l(H \cap A^t) + l(K) \leq l(H \cap A^t) + t - 1.$$

As $B \trianglelefteq H \cap A^t$, and B is the direct product of simple groups,

$$l(H \cap A^t) \leq l(B) + l((H \cap A^t)/B) \leq t + l((H \cap A^t)/B).$$

As A is almost simple, then $|(H \cap A^t)/B| \leq |\mathrm{Out}(S/Z(S))|^t$ and so we bound the chief length by

$$l((H \cap A^t)/B) \leq \log|\mathrm{Out}(S/Z(S))|^t \leq t\log|\mathrm{Out}(S/Z(S))|.$$

Then

$$l(H) \leq 2t + t\log|\mathrm{Out}(S/Z(S))| - 1.$$

We bound $|\mathrm{Out}(S/Z(S))|$ in two ways.

First note that $|S/Z(S)| \leq |S| \leq |\mathrm{GL}_s(q)| \leq q^{s^2}$. Then $|\mathrm{Out}(S/Z(S))| \leq (6/7)\log q^{s^2}$ and so

$$\log|\mathrm{Out}(S/Z(S))| \leq \log(6/7) + 2\log s + \log\log q.$$

Next we bound $|\mathrm{Out}(S/Z(S))|$ another way. As S embeds absolutely irreducibly in $\mathrm{GL}_s(q)$, then $Z(S) \leq Z(\mathrm{GL}_s(q))$ and so $S/Z(S)$ embeds in $\mathrm{PGL}_s(q)$. Then as $\mathrm{PGL}_s(q)$ has a permutation representation on $(q^s - 1)/(q-1) \leq q^s$ points, $S/Z(S)$ has a non-trivial permutation representation of degree at most q^s. As $S/Z(S)$ is simple, all non-trivial representations are faithful, and there must be a transitive permutation representation of degree at most q^s. Then, by Lemma 2.2.3, $|\mathrm{Out}(S/Z(S))| \leq 3\log q^s$, and so

$$\log|\mathrm{Out}(S/Z(S))| \leq \log 3 + \log s + \log\log q.$$

Then, using the fact that $l(H) \leq 2t + t\log|\mathrm{Out}(S/Z(S))| - 1$, we get our result. □

Lemma 11.1.13. *Let S be a quasisimple group that embeds absolutely irreducibly in $\mathrm{GL}_s(q)$, let A be an almost simple group with socle $S/Z(S)$, and let $B = (S/Z(S))^t$. Let $B \leq H \leq A \operatorname{wr} K$ for $K \leq S_t$. Further suppose that $s^t \leq 5$. Then $l(H)$ is bounded as follows.*

- *If $s = 2$ and $t = 1$, then $l(H) \leq 2.78 + \log\log q$.*
- *If $s = 2$ and $t = 2$, then $l(H) \leq 6.56 + 2\log\log q$.*
- *If $s = 3$ and $t = 1$, then $l(H) \leq 3.95 + \log\log q$.*
- *If $s = 4$ and $t = 1$, then $l(H) \leq 4.59 + \log\log q$.*
- *If $s = 5$ and $t = 1$, then $l(H) \leq 4.91 + \log\log q$.*

Proof. This follows immediately from the previous lemma. □

Using these bounds we now bound $l(G)$ for $G \leq \mathrm{GL}_n(q)$.

Lemma 11.1.14. *Let $G \leq \mathrm{GL}_n(q)$ where all abelian characteristic subgroups of G are contained in $Z(\mathrm{GL}_n(q))$. Suppose that $F^*(G)$ embeds absolutely irreducibly in $\mathrm{GL}_{n_1}(q_1)$ for some $2 \leq n_1 \leq n$ and some $q_1 \geq q$. Assume Theorem 11.0.4 holds in dimensions less than n. Then*

$$l(G/Z(G)) \leq 4\log n_1 + \log n_1 \log\log q_1$$

and

$$l(G) \leq 4\log n_1 + \log n_1 \log\log q_1 + \log(q-1).$$

Proof. Let $Z = Z(\mathrm{GL}_n(q))$, the set of scalar matrices. Then $Z \cap G \leq Z(G)$. As $Z(G)$ is an abelian characteristic subgroup then $Z(G) \leq Z$ by assumption. Then $Z \cap G = Z(G)$ and so $l(Z(G)) \leq \log(q-1)$. Combined with Lemma 9.1.15,

$$l(G) \leq l(G/Z(G)) + \log(q-1)$$

and so it remains to bound $l(G/Z(G))$.

We bound the chief length in terms of $n_1 \leq n$. Recall $F^*(G)$ can be described as a central product of non-central subgroups $O_{r_1}(G), \ldots, O_{r_c}(G)$, normal subgroups $T_1, \ldots, T_k$, where each T_i is a central product of $t_i \geq 1$ isomorphic copies of some subnormal quasisimple subgroup S_i, and $Z(G)$. It follows from Lemma 11.1.6 that $n_1 = x_1 \ldots x_c y_1 \ldots y_k$, where x_i is the dimension of some absolutely irreducible $O_{r_i}(G)$ module over $\mathbb{F}_{q_1}$, and y_i is the dimension of some absolutely irreducible T_i module over $\mathbb{F}_{q_1}$. It follows from Lemmas 11.1.7 and 11.1.8, that $x_i = r_i^{m_i}$ for some m_i, and $y_i = s_i^{t_i}$ where s_i is the dimension of some irreducible module for S_i. Then

$$n_1 = r_1^{m_1} \ldots r_c^{m_c} s_1^{t_1} \ldots s_k^{t_k}.$$

It follows from Lemma 2.0.26 that $C_G(F^*(G)) = Z(F^*(G))$, and as this is an abelian characteristic subgroup it is contained in $Z(\mathrm{GL}_n(q))$. Then $C_G(F^*(G)) = Z(G)$. By Lemma 11.1.3,

$$l(G/Z(G)) \leq \sum_{i=1}^{c} l(G/C_G(O_{r_i}(G))) + \sum_{i=1}^{k} l(G/C_G(T_i)).$$

First we bound $l(G/C_G(O_{r_i}(G)))$ and $l(G/C_G(T_i))$.

By Lemma 11.1.7, for primes r_i dividing $|G|$ such that $O_{r_i}(G)$ is non-central,

$$G/C_G(O_{r_i}(G)) \leq {r_i}^{2m_i}.\mathrm{Sp}_{2m_i}(r_i).$$

Then if $2m_i < n$, Lemma 11.1.10 applies and

$$l(G/C_G(O_{r_i}(G))) \leq 2m_i + 2\log r_i^{m_i}.$$

Otherwise if $2m_i \geq n$, then $2m_i \geq r_i^{m_i}$, and the only possibilities are $r_i = 2$ and $m_i = 1$ or 2. It follows from Lemma 11.1.11 that in these two cases $l(G/C_G(O_{r_i}(G)) \leq 2m_i + 2\log r_i^{m_i}$.

Next consider normal subgroups T_i which are central products of $t_i \geq 1$ copies of subnormal quasisimple groups S_i. Then if S_i has an irreducible module of dimension s_i, by Lemma 11.1.12

$$l(G/C_G(T_i)) \leq 2t_i + 2\log s_i^{t_i} + t_i \log\log q_1 - 1.$$

Recall $n_1 = r_1^{m_1} \dots r_c^{m_c} s_1^{t_1} \dots s_k^{t_k}$. Then,

$$\begin{aligned} l(G/Z(G)) &\leq \sum_{i=1}^{c}(2m_i + 2\log r_i^{m_i}) + \sum_{i=1}^{k}(2t_i + 2\log s_i^{t_i} + t_i\log\log q_1 - 1) \\ &\leq \sum_{i=1}^{c} 4\log r_i^{m_i} + \sum_{i=1}^{k}(4\log s_i^{t_i} + t_i\log\log q_1) \\ &= 4\log(r_1^{m_1}\dots r_c^{m_c}s_1^{t_1}\dots s_k^{t_k}) + \sum_{i=1}^{k} t_i\log\log q_1 \\ &\leq 4\log n_1 + \log n_1 \log\log q_1. \end{aligned}$$

It follows that $l(G) \leq 4\log n_1 + \log n_1 \log\log q_1 + \log(q-1)$. □

Next we show that the bound of $l(G) \leq n_1 + n_1 \log q_1 - 1$ also holds in this case. This is clearly true when n_1 is large enough, for smaller n_1 the proof uses the same ideas as above, but we are more careful with some calculations.

Lemma 11.1.15. *Let $G \leq \mathrm{GL}_n(q)$, where all abelian characteristic subgroups of G are contained in $Z(\mathrm{GL}_n(q))$. Suppose that $F^*(G)$ embeds absolutely irreducibly in $\mathrm{GL}_{n_1}(q_1)$ for some $n_1 \leq n$ and some $q_1 \geq q$. Suppose $n_1 \geq 6$. Assume Theorem 11.0.4 holds in dimensions less than n. Then*

$$l(G) \leq n_1 + n_1 \log q_1 - 1.$$

Proof. By Lemma 11.1.14,

$$l(G) \leq 4\log n_1 + \log n_1 \log\log q_1 + \log(q-1).$$

We will consider three cases: $q_1 = 2$, $q_1 = 3$ and $q_1 \geq 4$. Recall $q_1 \geq q$.

First suppose $q_1 = 2$. Then

$$\begin{aligned} l(G) &\leq 4\log n_1 + \log n_1 \log\log q_1 + \log(q-1) \\ &= 4\log n_1 \\ &\leq 2n_1 - 1 \\ &= n_1 + n_1 \log q_1 - 1, \end{aligned}$$

as required.

Next suppose that $q_1 = 3$. Then

$$\begin{aligned} l(G) &\leq 4\log n_1 + \log n_1 \log\log 3 + \log 2 \\ &\leq 4\log n_1 + (2/3)\log n_1 + 1 \\ &= (14/3)\log n_1 + 1 \\ &\leq (5/2)n_1 - 1 \\ &\leq n_1 + n_1 \log q_1 - 1. \end{aligned}$$

Finally suppose that $q_1 \geq 4$. Then $\log q_1 \geq 2$, and $\log\log q_1 \leq (\log q_1)/2$, and so

$$\begin{aligned} l(G) &\leq 4\log n_1 + \log n_1 \log\log q_1 + \log(q-1) \\ &\leq 4\log n_1 + (\log n_1 \log q_1)/2 + \log q_1 \\ &= 4\log n_1 + (\log n_1/2 + 1)\log q_1 \\ &\leq 2\log n_1 + (3\log n_1/2 + 1)\log q_1 \\ &\leq n_1 + (n_1 - 1)\log q_1 \\ &\leq n_1 + n_1 \log q_1 - 1. \end{aligned}$$

Thus for $n \geq 6$ and all q_1,

$$l(G) \leq n_1 + n_1 \log q_1 - 1.$$

□

Lemma 11.1.16. *Let $G \leq \mathrm{GL}_n(q)$, where all abelian characteristic subgroups of G are contained in $Z(\mathrm{GL}_n(q))$. Suppose that $F^*(G)$ embeds absolutely irreducibly in $\mathrm{GL}_{n_1}(q_1)$ for some $2 \leq n_1 \leq n$ and some $q_1 \geq q$. Assume Theorem 11.0.4 holds in dimensions less than n. Then*

$$l(G) \leq n_1 + n_1 \log q_1 - 1.$$

Proof. If $n_1 \geq 6$ then the bound holds by Lemma 11.1.15.

For the remainder of the proof $2 \leq n_1 \leq 5$. We use the same arguments and notation as the proof of Lemma 11.1.14. Again $Z(G) = Z(\mathrm{GL}_n(q))$. As

$l(Z(G)) \leq \log(q-1)$, then by Lemma 9.1.15, $l(G) \leq l(G/Z(G)) + \log(q-1)$. By Lemma 11.1.3

$$l(G/Z(G)) \leq \sum_{i=1}^{c} l(G/C_G(O_{r_i}(G))) + \sum_{i=1}^{k} l(G/C_G(T_i)).$$

As $n_1 \leq 5$, the dimension $n_1 = r_1^{m_1} r_2^{m_2} s_1^{t_1} s_2^{t_2}$, that is, $c \leq 2$ and $k \leq 2$, and we consider all possibilities for r_i, m_i, s_i, t_i.

If $n_1 = 2$, then either $c = 1$ and $k = 0$, or $c = 0$ and $k = 1$. Then it follows from Lemmas 11.1.11 and 11.1.13 that

$$l(G) \leq \max\{4 + \log(q-1), 2.78 + \log\log q_1 + \log(q-1)\}.$$

If $q_1 \geq 4$, then $l(G) \leq 2 + 2\log q_1 - 1$ as required. Using MAGMA we may calculate the chief length of all subgroups of $\mathrm{GL}_2(2)$ and $\mathrm{GL}_2(3)$. If $G \leq \mathrm{GL}_2(2)$ then $l(G) \leq 2$, and if $G \leq \mathrm{GL}_2(3)$ then $l(G) \leq 3$. Thus if $n_1 = 2$, then the bound $l(G) \leq n_1 + n_1 \log q_1 - 1$ holds for all q_1.

If $n_1 = 3$ then either $c = 1$ and $k = 0$, or $c = 0$ and $k = 1$. By Lemmas 11.1.11 and 11.1.13,

$$l(G) \leq \max\{5 + \log(q-1), 3.95 + \log\log q_1 + \log(q-1)\}.$$

Then if $n_1 = 3$, the bound holds.

If $n_1 = 5$ then either $c = 1$ and $k = 0$, or $c = 0$ and $k = 1$. It follows from Lemmas 11.1.11 and 11.1.13 that

$$l(G) \leq \max\{5 + \log(q-1), 4.91 + \log\log q_1 + \log(q-1)\}.$$

Then the bound holds when $n_1 = 5$.

Finally, if $n_1 = 4$ we have the following possibilities: $c = 1$, $k = 1$, $r_1 = 2$, $m_1 = 2$, $s_1 = 2$ and $t_1 = 1$; $c = 1$, $k = 0$, $r_1 = 2$ and $m_1 = 2$; $c = 0$, $k = 1$, $s_1 = 2$ and $t_1 = 2$; $c = 0$, $k = 1$, $s_1 = 4$ and $t_1 = 1$; $c = 0$, $k = 2$, $s_1 = 2$, $t_1 = 1$, $s_2 = 2$ and $t_2 = 2$. By Lemmas 11.1.11 and 11.1.13,

$$l(G) \leq \max\{6.78 + 2\log\log q_1 + \log(q-1), 8 + \log(q-1)\}.$$

So for $n_1 = 4$, if $q_1 \geq 3$, then $l(G) \leq n_1 + n_1 \log q_1 - 1$. For $q_1 = 2$, then using MAGMA we calculate the chief length of all subgroups of $\mathrm{GL}_4(2)$. In this case if $G \leq \mathrm{GL}_4(2)$, then $l(G) \leq 6$. Then for $n_1 = 4$ and all q_1, the bound $l(G) \leq n_1 + n_1 \log q_1 - 1$ holds.

Then for all n_1, the bound $l(G) \leq n_1 + n_1 \log q_1 - 1$ holds. □

Lemma 11.1.17. *Let $G \leq \mathrm{GL}_n(q)$ be a weakly quasiprimitive group of dimension $n \geq 2$, where all abelian characteristic subgroups of G are contained in $Z(\mathrm{GL}_n(q))$. Assume Theorem 11.0.4 holds in dimensions less than n. Then*

$$l(G) \leq \min\{(\log n)^2/4 + 4\log n + \log n \log\log q + \log(q-1), n + n\log q - 1\}.$$

Proof. Let $V = \mathbb{F}_q^n$, the natural module for G. All abelian characteristic subgroups of G are contained in $Z(\mathrm{GL}_n(q))$ and so $Z(G) = Z(\mathrm{GL}_n(q)) \cap G$. Then $l(Z(G)) \leq \log(q-1)$. By Lemma 9.1.15, $l(G) = l(Z(G)) + l(G/Z(G))$ and so it remains to calculate $l(G/Z(G))$.

As $F^*(G)$ is a characteristic subgroup of G and G is weakly quasiprimitive, then $F^*(G)$ acts homogeneously on V. So $F^*(G)$ acts irreducibly and faithfully on $V = V_1 \oplus \ldots \oplus V_t$ for some $V_i \cong V_1$. Then $F^*(G)$ acts irreducibly and faithfully on each constituent V_i, that is $F^*(G)$ is an irreducible subgroup of $\mathrm{GL}_{n/t}(q)$.

First suppose that $\mathbb{F}_q$ is a splitting field for $F^*(G)$. Then the result follows from Lemmas 11.1.14 and 11.1.16 by taking $n_1 = n/t$, $q_1 = q$, and noting that $t \geq 1$.

Now suppose that $\mathbb{F}_q$ is not a splitting field for $F^*(G)$. By Theorem 2.2.12, $F^*(G)$ embeds irreducibly into $\mathrm{GL}_{n_1}(q_1)$ where $n_1 = n/tf$ and $q_1 = q^f$ for some f, and $\mathbb{F}_{q^f}$ is a splitting field for $F^*(G)$. Then, by Lemma 11.1.14, and using the fact that $t \geq 1$,

$$l(G/Z(G)) \leq 4\log n_1 + \log n_1 \log\log q_1.$$

Lemma 2.4.3 tells us that $(\log f)(\log(n/f))$ is largest when $f = \sqrt{n}$. Then

$$\begin{aligned} l(G/Z(G)) &\leq 4\log(n/f) + \log(n/f)\log\log q^f \\ &\leq 4\log(n/f) + \log(n/f)(\log f + \log\log q) \\ &\leq (\log n)^2/4 + 4\log n + \log n \log\log q. \end{aligned}$$

Then

$$l(G) \leq (\log n)^2/4 + 4\log n + \log n \log\log q + \log(q-1).$$

Similarly, by Lemma 11.1.16,

$$\begin{aligned} l(G) &\leq n_1 + n_1 \log q_1 - 1 \\ &\leq (n/f) + (n/f)\log q^f - 1 \\ &\leq n + n\log q - 1. \end{aligned}$$

□

Lemma 11.1.18. *Let $G \leq \mathrm{GL}_n(q)$ be a weakly quasiprimitive group where $n \geq 2$ and assume Theorem 11.0.4 holds in dimensions less than n. Then*

$$l(G) \leq \min\{(\log n)^2/2 + 4\log n + n\log q, n + n\log q - 1\}.$$

Proof. If all abelian characteristic subgroups of G are contained in $Z(\mathrm{GL}_n(q))$ then the result holds by Lemma 11.1.17.

So for the remainder of the proof assume there exists an abelian characteristic subgroup not contained in $Z(\mathrm{GL}_n(q))$. As G is a characteristic

subgroup of itself it is homogeneous and acts faithfully on each of its constituents. Thus we may assume that G is irreducible. By Lemma 11.1.9 there exists a characteristic subgroup K of G which is not contained in $Z(\mathrm{GL}_n(q))$ such that $K \cong K_1 \leq \mathrm{GL}_{n_1}(q_1)$ for $n_1 = n/f$, $q_1 = q^f$, and $f \geq 2$. Here K_1 is weakly quasiprimitive and all its characteristic abelian subgroups are contained in $Z(\mathrm{GL}_{n_1}(q_1))$. Furthermore, G/K is abelian of order at most f. Then by Lemma 9.1.15,

$$l(G) \leq l(K) + l(G/K) \leq l(K_1) + \log f.$$

Lemma 11.1.17 allows us to bound $l(K_1)$ as $n_1 < n$. Again we will use Lemma 2.4.3 to show $\log(n/f)\log f$ is largest when $f = \sqrt{n}$. Then $l(K_1)$ is bounded as follows

$$\begin{aligned} l(K_1) &\leq (\log n_1)^2/4 + 4\log n_1 + \log n_1 \log\log q_1 + \log(q_1 - 1) \\ &\leq (\log(n/f))^2/4 + 4\log(n/f) + \log(n/f)\log\log q^f + \log(q^f - 1) \\ &\leq (\log n)^2/4 + (\log\sqrt{n})^2 + n\log q + 4\log(n/f) \\ &\leq (\log n)^2/2 + n\log q + 4\log(n/f). \end{aligned}$$

Then we bound $l(G)$,

$$\begin{aligned} l(G) &\leq l(K_1) + \log f \\ &\leq (\log n)^2/2 + n\log q + 4\log(n/f) + \log f \\ &\leq (\log n)^2/2 + 4\log n + n\log q. \end{aligned}$$

Similarly, we may bound $l(K_1) \leq n_1 + n_1 \log q_1 - 1$ and thus

$$\begin{aligned} l(G) &\leq n_1 + n_1\log q_1 - 1 + \log f \\ &\leq (n/f) + (n/f)\log q^f - 1 + \log f \\ &\leq n + n\log q - 1. \end{aligned}$$

□

11.2 The chief length of completely reducible matrix groups

Now we may extend these results to bound $l(G)$ for completely reducible matrix groups and thus prove Theorem 11.0.4. Recall a primitive matrix group is necessarily weakly quasiprimitive.

Proof of Theorem 11.0.4. We prove this by induction on the dimension n. When $n = 1$, the bound holds by Lemma 11.0.5. Then assume that $n > 1$, and that the bound holds in dimensions less than n.

Using this inductive assumption, by Lemma 11.1.18, if G is weakly quasiprimitive, then

$$l(G) \leq \min\{n + n\log q - 1, (\log n)^2/2 + 4\log n + n\log q\}.$$

In particular, as all primitive groups are weakly quasiprimitive then $l(G) \leq n + n\log q - 1$ for primitive groups G.

Next suppose that G is reducible, that is $V = V_1 \oplus \cdots \oplus V_s$ as a sum of irreducible subspaces V_i, where $s \geq 2$. Then G is a subdirect product of $G_1 \times \cdots \times G_s$ where $G_i \leq \mathrm{GL}(V_i) = \mathrm{GL}_{n_i}(q)$ is irreducible and $n = n_1 + \cdots + n_s$. As G_i has dimension $n_i < n$, then $l(G_i) \leq n_i + n_i \log q - 1$ by induction. By Lemma 9.1.19,

$$\begin{aligned} l(G) &\leq l(G_1) + \cdots + l(G_s) \\ &\leq n + n\log q - s \end{aligned}$$

as required.

Finally suppose G is imprimitive, that is, G is irreducible but preserves some direct sum decomposition $V = V_1 \oplus \cdots \oplus V_k$ where $V_1 \cong V_i$ for $1 \leq i \leq k$ and $\dim(V_i) = m$. Then by Theorem 2.1.15 $G \leq H \operatorname{wr} K$ for some $H \leq \mathrm{GL}_m(q)$, $K \leq S_k$ and $n = mk$. As $H^k \cap G$ is normal in G, it is a completely reducible subgroup of G. As $H \leq \mathrm{GL}_m(q)$, H^k acts on a direct sum of at least k irreducible subspaces and it follows that $H^k \cap G$ is a completely reducible subgroup where V is the direct sum of at least k irreducible subspaces V_i. By the reducible subgroup case above

$$l(H^k) \leq n + n\log q - k.$$

As K is a permutation group of degree k then $l(K) \leq k - 1$. As

$$G/(H^k \cap G) \cong K$$

then by Lemma 9.1.15

$$l(G) \leq l(H^k \cap G) + l(K) \leq n + n\log q - 1.$$

□

Although this bound is not known to be tight, we construct examples which are close to achieving the bounds on the chief length from this theorem.

Example 11.2.1. Consider subgroups of the form $\Gamma\mathrm{L}_1(p^n)$ in $\mathrm{GL}_n(p)$ where p and n are primes (these are maximal subgroups lying in Aschbacher class $\mathcal{C}_3$). The subgroup $\Gamma\mathrm{L}_1(p^n) = (p^n - 1) : n$ is a quasiprimitive subgroup of $\mathrm{GL}_n(p)$. Then if $(p^n - 1)$ is a power of 2,

$$l(\Gamma\mathrm{L}_1(p^n)) = \log(p^n - 1) + 1 \simeq n\log p + 1.$$

Example 11.2.2. Consider the group $G = \mathrm{GL}_1(q)$, where $(q-1)$ is a power of 2. Then $l(G) = \log(q-1)$. Then G^n is a completely reducible subgroup of $\mathrm{GL}_n(q)$ which acts on $V_1 \oplus \cdots \oplus V_n$ for $V_i \cong \mathbb{F}_q$, with each V_i irreducible. Then by Lemma 9.1.16,

$$l(G^n) = nl(G) = n\log(q-1).$$

This is close to achieving the bound on the chief length from Theorem 11.0.4, which in this case is

$$l(G^n) \leq n + n\log q - n = n\log q.$$

11.3 Random generation of completely reducible matrix groups

Now we can use the bound on the chief length of completely reducible matrix groups to improve the results for random generation when G is a completely reducible and when it is weakly quasiprimitive. When G is completely reducible $d(G) \leq 3n/2$ by Theorem 9.2.13 and when G is weakly quasiprimitive $d(G) \leq 2\log n + 1$ from Theorem 9.2.14. Then using Theorem 9.2.4 we get the following bounds on $d^\epsilon(G)$.

Theorem 11.3.1. *Let $\epsilon \in (0,1)$ and let t be such that $\zeta(t) \leq 1+\epsilon$. Let $G \leq \mathrm{GL}_n(q)$ be a completely reducible matrix group. Then*

$$d^\epsilon(G) \leq 3n/2 + 2\log(n + n\log q - 1) + t + 2.$$

If G is weakly quasiprimitive then

$$d^\epsilon(G) \leq 2\log n + 2\log((\log n)^2/2 + 4\log n + n\log q) + t + 3.$$

11.4 Further work

Recall our initial motivation for studying random generation: its application to constructing composition trees. In this case we are given a permutation or matrix group G, and we are constructing subnormal subgroups N (which are kernels of homomorphisms) by random generation. Thus we would ideally like to estimate $d^\epsilon(G)$ for $N \lhd\lhd G$. If G is a permutation group of degree n acting on s orbits, then any $N \lhd\lhd G$ is a permutation group of degree n acting on at least s orbits. Similarly for G a completely reducible group, all normal subgroups, and hence all subnormal subgroups are completely reducible. In these 2 cases, our bounds on $d^\epsilon(G)$ are in fact upper bounds on $d^\epsilon(N)$ for $N \lhd\lhd G$.

There are tighter bounds on $d(G)$ and $l(G)$, and hence $d^\epsilon(G)$ for G a primitive permutation groups or a weakly quasiprimitive matrix groups.

The bounds on $d(G)$ in fact hold for subnormal subgroups of G in these cases, and we would like to extend our bounds on $l(G)$ so they hold for all subnormal subgroups of such G. Then we would have tighter bounds on $d^e(N)$ for $N \lhd\lhd G$ in these cases. Note that the bound on $c(G)$ (the composition length of G) for primitive groups G, is in fact an upper bound on the chief length for subnormal subgroups N of G.

Recall the Frattini subgroup of a group G, $\Phi(G)$, is the intersection of all maximal subgroups of G. If N_{i+1}/N_i is a chief factor of G, and $N_{i+1}/N_i \leq \Phi(G/N_i)$, then N_{i+1}/N_i is a Frattini chief factor of G. Let $\lambda(G)$ denote the non-Frattini chief length of G, that is, the number of non-Frattini chief factors of G. Then $l(G)$ may be replaced by $\lambda(G)$ in Theorem 9.2.4, and in some cases this may give a tighter bound on $d^e(G)$ as $\lambda(G) \leq l(G)$. However, in some of the cases we consider, it is not that useful. Consider $\mathrm{GL}_1(q)$, where $(q-1)$ is the product of distinct primes. Then $\Phi(G) = 1$ and so in this case $\lambda(G) = l(G)$.

Bibliography

[1] M. Aschbacher (1986), *Finite Group Theory*, Cambridge University Press.

[2] M. Aschbacher (1984), On the maximal subgroups of the finite classical groups, *Invent. Math.* **76**, 469–514.

[3] Michael Aschbacher & Gary M. Seitz (1976), Involutions in Chevalley groups over fields of even order, *Nagoya Math. J.* **63**, 1–91; correction, *ibid.* **72** (1978), 135–136.

[4] László Babai (1989), The probability of generating the symmetric group, *J. Combin. Th. Ser. A* **52**, 148–153.

[5] Meenaxi Bhattacharjee (1994), The probability of generating certain profinite groups by two elements, *Isr. J. Math.* **86**, 311–329.

[6] M. Bhattacharjee, R.G. Möller, D. Macpherson, P.M. Neumann (1997), *Notes on infinite permutation groups*, Hindustan Book Agency.

[7] John Bovey & Alan Williamson (1978), The probability of generating the symmetric group, *Bull. London Math. Soc.* **10**, 91–96.

[8] Wieb Bosma, John Cannon, and Catherine Playoust (1997), The Magma algebra system. I. The user language. *J. Symbolic Comput.*, **24(3-4)**, 235–265.

[9] J.N. Bray, personal communication.

[10] John N. Bray, Derek F. Holt & Colva M. Roney-Dougal, *The maximal subgroups of the low dimensional finite classical groups*, London Mathematical Society Lecture Note Series, CUP, to appear.

[11] Peter J. Cameron (1999), *Permutation Groups*, CUP.

[12] Peter J. Cameron (1981), Finite permutation groups and finite simple groups, *Bull. London Math. Soc.* **13**, 1–22.

[13] Peter J. Cameron, Ron Solomon & Alexandre Turull (1989), Chains of subgroups in symmetric groups, *J. Algebra* **127**, 340–352.

[14] Roger W. Carter (1972), *Simple Groups of Lie Type*, John Wiley & Sons.

[15] Roger Carter & Paul Fong (1964), The Sylow 2-subgroups of the finite classical groups, *J. Algebra* **1**, 139–151.

[16] Arjeh M. Cohen, Martin W. Liebeck, Jan Saxl & Gary M. Seitz (1992), The local maximal subgroups of exceptional groups of Lie type, finite and algebraic, *Proc. London Math. Soc.* **64**, 21–48.

[17] J.H. Conway, R. A. Curtis, S.P. Norton, R.A. Parker, R.A. Wilson (1985), Atlas *of Finite Groups*, OUP.

[18] Bruce N. Cooperstein (1978), Minimal degree for a permutation representation of a classical group, *Isr. J. Math* **30**, 213–235.

[19] Bruce N. Cooperstein (1981), Maximal subgroups of $G_2(2^n)$, *J. Algebra* **70**, 23–36.

[20] Francesca Dalla Volta & Andrea Lucchini (1995), Generation of almost simple groups, *J. Algebra* **178**, 194–223.

[21] Eloisa Detomi & Andrea Lucchini (2012), Probabilistic generation of finite groups with a unique minimal normal subgroup, *to appear*.

[22] John D. Dixon (1969), The probability of generating the symmetric group, *Math. Z.* **110**, 199–205.

[23] John D. Dixon (2005), Asymptotics of generating the symmetric and alternating groups, *Electron. J. Combin.* **12**, Research paper 56.

[24] John D. Dixon & Brian Mortimer (1996), *Permutation Groups*, Springer-Verlag.

[25] P. Erdös & P. Turán (1967), On some problems of a statistical group theory II, *Acta Math. Acad. Sci. Hung.* **18**, 151–163.

[26] Walter Feit & John G. Thompson (1963), Solvability of groups of odd order, *Pacific J. Math.* **13**, 775–1029.

[27] R.K. Fisher (1974), The polycyclic length of linear and finite polycyclic groups, *Can. J. Math.* **4**, 1002–1009.

[28] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.4.12*, (2008), (`http://www.GAP-system.org`).

[29] W.Gashütz (1955), Zu einem von B.H. und H. Neumann gestellten Problem, *Math. Nachr.* **14**, 249–252.

[30] Daniel Gorenstein (1968), *Finite Groups*, Harper & Row.

[31] Robert M. Guralnick, William M. Kantor & Jan Saxl (1994), The probability of generating a classical group, *Comm. Algebra* **22**, 1395–1402.

[32] P. Hall (1936), The Eulerian functions of a group, *Quart. J. Math.* **7**, 134–151.

[33] Jokke Häsä (2011), Growth of cross-characteristic representations of finite quasisimple groups of Lie type, arXiv:1112.3941v1.

[34] Gerhard Hiss & Gunter Malle (2001), Low-dimensional representations of quasi-simple groups, *LMS J. Comput. Math.* **4**, 22–63.

[35] Derek F. Holt & Colva M. Roney-Dougal (2011), Minimal and random generation of permutation and matrix groups, *to appear*.

[36] I. Martin Isaacs (1976), *Character Theory of Finite Groups*, Academic Press, Inc. (London) Ltd.

[37] Nagayoshi Iwahori (1970), Centralizers of involutions in finite Chevalley groups, *Seminar on Algebraic Groups and Related Topics, Lecture Notes in Math.*, Springer, 267–295.

[38] Andrei Jaikin-Zapirain & Lázló Pyber (2011), Random generation of finite and profinite groups and group enumeration, *Ann. of Math.* **173**, 769–814.

[39] Christoph Jansen, K. Lux, R Parker and R Wilson (1995), *An* Atlas *of Brauer Characters*, Clarendon Press.

[40] William M. Kantor & Alexander Lubotzky (1990), The probability of generating a finite classical group, *Geom. Dedicata* **36**, 67–87.

[41] W. Kimmerle, R. Lyons, R. Sandling, D. N. Teague (1990), Composition factors from the group ring and Artin's theorem on orders of simple groups, *Proc. London Math. Soc* **60**, 89–122.

[42] Peter B. Kleidman (1988), The maximal subgroups of the Steinberg triality groups ${}^3\mathrm{D}_4(q)$ and of their automorphism groups, *J. Algebra* **115**, 182–199.

[43] Peter B. Kleidman (1988), The maximal subgroups of the Chevalley groups $\mathrm{G}_2(q)$ with q odd, the Ree groups ${}^2\mathrm{G}_2(q)$, and their automorphism groups, *J. Algebra* **117**, 30–71.

[44] Peter Kleidman & Martin Liebeck (1990), *The Subgroup Structure of the Finite Classical Groups*, London Math. Soc. Lecture Note Ser., CUP.

[45] Peter B. Kleidman & Robert A. Wilson (1990), The maximal subgroups of $E_6(2)$ and $\mathrm{Aut}(E_6(2))$, *Proc. London Math. Soc.* **60**, 266–294.

[46] Peter B. Kleidman & Robert A. Wilson (1993), Sporadic simple subgroups of finite exceptional groups of Lie type, *J. Algebra* **157**, 316–330.

[47] L.G. Kovács & G.R. Robinson (1991), Generating finite completely reducible linear groups, *Proc. Amer. Math. Soc* **112**, 357–364.

[48] A. Languasco, F. Menegazzo & M. Morigi (2002), On the composition length of finite primitive linear groups, *Arch. Math.* **79**, 408–417.

[49] Vincente Lanzaduri & Gary M. Seitz (1974), On the minimal degrees of projective representations, *J. Algebra* **32**, 418–443.

[50] Walter Ledermann (1977), *Introduction to group characters*, CUP.

[51] Martin W. Liebeck (1985), On the orders of maximal subgroups of the finite classical groups, *Proc. London Math. Soc.* **50**, 426–446.

[52] Martin W. Liebeck (1984), On minimal degrees and base sizes of primitive permutation groups, *Arch. Math.* **43**, 11–15

[53] Martin W. Liebeck, Cheryl E. Praeger & Jan Saxl (1987), A classification of the maximal subgroups of the finite alternating and symmetric groups, *J. Algebra* **111**, 365–383.

[54] Martin W. Liebeck & Jan Saxl (1987), On the orders of maximal subgroups of the finite exceptional groups of Lie type, *Proc. London Math. Soc.*, **55**, 299–330.

[55] Martin W. Liebeck, Jan Saxl & Gary M. Seitz (1992), Subgroups of maximal rank in finite exceptional groups of Lie type, *Proc. London Math. Soc.*, **65**, 297–325.

[56] Martin W. Liebeck, Jan Saxl & Donna M. Testerman (1996) , Simple subgroups of large rank in groups of Lie type, *Proc. London Math. Soc.*, **72**, 425–257.

[57] Martin W. Liebeck & Gary M. Seitz (1990), Maximal subgroups of exceptional groups of Lie type, finite and algebraic, *Geom. Dedicata*, **35**, 353–387.

[58] Martin W. Liebeck & Gary M. Seitz (1994), Subgroups generated by root elements in groups of Lie type, *Ann. Math.*, **139**, 293–361.

[59] Martin W. Liebeck & Gary M. Seitz (2003), A survey of maximal subgroups of exceptional groups of Lie type, *Groups, Combinatorics and Geometry: Durham, 2001*, World Scientific, 139–146.

[60] Martin W. Liebeck & Gary M. Seitz (1999), On finite subgroups of exceptional algebraic groups, *J. Reine Angew. Math.* **515**, 25–72.

[61] Martin W. Liebeck & Gary M.Seitz (2005), Maximal subgroups of large rank in exceptional groups of Lie type, *J. London Math. Soc.* **71**, 345–361.

[62] Martin W. Liebeck & Aner Shalev (1995), The probability of generating a finite simple group, *Geom. Dedicata* **56**, 103–113.

[63] Frank Lübeck (2001), Small degree representations of finite Chevalley groups in defining characterisitic, *LMS J. Comput. Math.* **4**, 135–169.

[64] Alexander Lubotzky (2002), The expected number of random elements to generate a finite group, *J. Algebra* **257**, 452–459.

[65] A. Lucchini, F. Menegazzo & M. Morigi (2001), On the number of generators and composition length of finite linear groups, *J. Algebra* **243**, 427–447.

[66] Andrea Lucchini & Fiorenza Morini (2002), On the probability of generating finite simple groups with a unique minimal normal subgroup, *Pacific J. Math.* **203**, 429–440.

[67] K. Magaard (1990), *The maximal subgroups of the Chevalley groups* $\mathrm{F}_4(F)$ *where* F *is a finite or algebraically closed field of characteristic* $\neq 2, 3$*,* Ph.D. thesis, Calif. Inst. Tech.

[68] Gunter Malle (1991), The maximal subgroups of ${}^2\mathrm{F}_4(q^2)$, *J. Algebra* **139**, 52–69.

[69] Gunter Malle, Jan Saxl & Thomas Weigel (1994), Generation of classical groups, *Geom. Dedicata* **49**, 85–116.

[70] Attila Maróti & M. Chiara Tamburini (2011), Bounds for the probability of generating the symmetric and alternating groups, *Arch. Math* **96**, 115–121.

[71] V. D. Mazurov & E. I. Khukhro (eds.) (2010), *The Kourovka Notebook, No. 17*, Russian Academy of Sciences, Institute of Mathematics, Novosibirsk.

[72] U. Meierfrankenfeld & S. Shpectorov (2002 & 2003), Maximal 2-local subgroups of the Monster and Baby Monster, I & II, preprints (`http://www.math.msu.edu/~meier/Preprints/2monster/abstract.html`).

[73] Nina E. Menezes, Martyn Quick & Colva M. Roney-Dougal (2012), The probability of generating a finite simple group, *Isr. J. Math*, *to appear*.

[74] L. Naughton & G.Pfeiffer, Tomlib, Version 1.2.1, GAP package, (2011), (`http://schmidt.nuigalway.ie/tomlib`).

[75] E. Netto (1892), *The Theory of Substitutions*, Ann. Arbor Mich.

[76] S. P. Norton & R. A. Wilson (1989), The maximal subgroups of $F_4(2)$ and its automorphism group, *Comm. Algebra* **17**, 2809–2824.

[77] Simon P. Norton & Robert A. Wilson (2002), Anatomy of the Monster: II, *Proc. London Math. Soc.* **3**, 581–598.

[78] Igor Pak (1999), On probability of generating a finite group, preprint.

[79] László Pyber (1993), Asymptotic results for permutation groups, *DIMACS Ser. in Discrete Math. Theoret. Comput. Sci.* **11**, 197–219.

[80] László Pyber (1997), Asymptotic results for simple groups and some applications, *DIMACS Ser. in Discrete Math. Theoret. Comput. Sci.* **28**, 309–327.

[81] Martyn Quick (2004), Probabilistic generation of wreath products of non-abelian finite simple groups, *Comm. Algebra*, **32**, 4753–4768.

[82] Luis Ribes & Pavel Zalesskii (2000), *Profinite groups*, Springer.

[83] John S. Rose (1978), *A Course on Group Theory*, CUP.

[84] Walter Rudin (1976), *Principles of Mathematical Analysis*, McGraw Hill.

[85] L. Scott (1980), Representations in characteristic p, *Proc. Sympos. Pure Math.* **37**, 319–332.

[86] Michio Suzuki (1962), On a class of doubly transitive groups, *Ann. Math.* **75**, 105–145.

[87] Donald E. Taylor (1992), *The Geometry of the Classical Groups*, Helderman Verlag, Berlin.

[88] A.V. Vasilyev (1996), Minimal permutation representations of finite simple exceptional groups of types G_2 and F_4, *Algebra and Logic* **35**, 371–383.

[89] A.V. Vasilyev (1997), Minimal permutation representations of finite simple exceptional groups of types E_6, E_7, and E_8, *Algebra and Logic* **36**, 302–310.

[90] A.V. Vasilyev (1998), Minimal permutation representations of finite simple exceptional twisted groups, *Algebra and Logic* **37**, 9–20.

[91] Robert A. Wilson (1988), The odd-local subgroups of the Monster, *J. Austral. Math. Soc. (Series A)* **44**, 1–16.

[92] Robert A. Wilson (2009), *The Finite Simple Groups*, Springer.

[93] Robert A. Wilson, Personal communication.

[94] Robert Wilson et al., ATLAS of Finite Group Representations Version 3, (`http://brauer.maths.qmul.ac.uk/ATLAS/v3/`)

[95] Ascher Wagner (1977), An observation on the degrees of projective representations of the symmetric and alternating groups over an arbitrary field, *Arch. Math* **29**, 583–589.